NAVAL POSTGRADUATE SCHOOL

MONTEREY, CALIFORNIA

THESIS

SYSTEM OF SYSTEMS TECHNOLOGY READINESS ASSESSMENT

by

WindyJoy S. Majumdar

September 2007

Thesis Advisor:	John Osmundson
Co-Advisor:	Jay Mandelbaum

Approved for public release; distribution is unlimited

THIS PAGE INTENTIONALLY LEFT BLANK

REPORT DOCUMENTATION PAGE	*Form Approved OMB No. 0704-0188*

1. AGENCY USE ONLY *(Leave blank)*	**2. REPORT DATE** September 2007	**3. REPORT TYPE AND DATES COVERED** Master's Thesis

4. TITLE AND SUBTITLE System of Systems Technology Readiness Assessment	**5. FUNDING NUMBERS**
6. AUTHOR(S) Majumdar, WindyJoy S.	
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) Naval Postgraduate School Monterey, CA 93943-5000	**8. PERFORMING ORGANIZATION REPORT NUMBER**
9. SPONSORING /MONITORING AGENCY NAME(S) AND ADDRESS(ES) N/A	**10. SPONSORING/MONITORING AGENCY REPORT NUMBER**

11. SUPPLEMENTARY NOTES The views expressed in this thesis are those of the author and do not reflect the official policy or position of the Department of Defense or the U.S. Government.

12a. DISTRIBUTION / AVAILABILITY STATEMENT Approved for public release; distribution is unlimited.	**12b. DISTRIBUTION CODE**

13. ABSTRACT (maximum 200 words)

The Chairman of the Joint Chiefs of Staff established the Joint Capabilities Integration and Development System processes for acquisition of joint capabilities which are achieved through network-centric applications, services, enterprise systems, Family of Systems (FoS) and System of Systems (SoS). In many cases, advanced technologies must be matured simultaneously by multiple systems to support the degree of interoperability and/or integration required. Current DoD guidance with respect to technology development and assessment is focused on a acquisition of a system which operates relatively independently within a collection of other independent systems.

An approach to technology development and technology readiness assessment of advanced technologies which support network-centric systems is required for successful development and fielding of network centric warfighting capabilities**.** Fundamental activities of technology maturation and assessments are the definition of a relevant environment and the ability to identify the critical technologies that provide for interoperable or interdependent functions. This paper proposes definitions for System of Systems and Family of Systems, degrees/levels of interoperability, and SoS Technology Readiness Assessment requirements and guidelines. SoS acquisition strategies are proposed to support program synchronization and SoS engineering activities which are key to successful development of net-centric Service and Joint capabilities.

14. SUBJECT TERMS System of Systems, Technology Readiness Assessment, Family of Systems, Technology Readiness Level	**15. NUMBER OF PAGES** 165
	16. PRICE CODE

17. SECURITY CLASSIFICATION OF REPORT Unclassified	**18. SECURITY CLASSIFICATION OF THIS PAGE** Unclassified	**19. SECURITY CLASSIFICATION OF ABSTRACT** Unclassified	**20. LIMITATION OF ABSTRACT** UU

THIS PAGE INTENTIONALLY LEFT BLANK

Approved for public release; distribution is unlimited

SYSTEM OF SYSTEMS TECHNOLOGY READINESS ASSESSMENT

WindyJoy S. Majumdar
Civilian, Department of Navy
B.S., University of Tennessee, 1984

Submitted in partial fulfillment of the
requirements for the degree of

MASTER OF SCIENCE IN SYSTEM ENGINEERING MANAGEMENT

from the

NAVAL POSTGRADUATE SCHOOL
September 2007

Author: WindyJoy Springs Majumdar

Approved by: John Osmundson, Ph.D
Thesis Advisor

Jay Mandelbaum, D.Sc.
Co-Advisor

David H. Olwell, Ph.D.
Chairman, Department of Systems Engineering

THIS PAGE INTENTIONALLY LEFT BLANK

ABSTRACT

The Chairman of the Joint Chiefs of Staff established the Joint Capabilities Integration and Development System processes for acquisition of joint capabilities which are achieved through network-centric applications, services, enterprise systems, Family of Systems (FoS) and System of Systems (SoS). In many cases, advanced technologies must be matured simultaneously by multiple systems to support the degree of interoperability and/or integration required. Current DoD guidance with respect to technology development and assessment is focused on a acquisition of a system which operates relatively independently within a collection of other independent systems.

An approach to technology development and technology readiness assessment of advanced technologies which support network-centric systems is required for successful development and fielding of network centric warfighting capabilities. Fundamental activities of technology maturation and assessments are the definition of a relevant environment and the ability to identify the critical technologies that provide for interoperable or interdependent functions. This paper proposes definitions for System of Systems and Family of Systems, degrees/levels of interoperability, and SoS Technology Readiness Assessment requirements and guidelines. SoS acquisition strategies are proposed to support program synchronization and SoS engineering activities which are key to successful development of net-centric Service and Joint capabilities.

THIS PAGE INTENTIONALLY LEFT BLANK

TABLE OF CONTENTS

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF FIGURES

LIST OF TABLES

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF SYMBOLS, ACRONYMS, AND/OR ABBREVIATIONS

ACAT	Acquisition Category
AF	Air Force
AIAMD SOS	Army’s Integrated Air and Missile Defense System of Systems
AOC	Air Operations Center
APB	Acquisition Program Baseline
APRANET	Advance Research Program Agency wide-area networking
ASN(RDA)	Assistance Secretary of the Navy (Research, Development and Acquisition)
ATM	Asynchronous Transfer Mode
ATO	Air Tasking Order
B	Both Hardware and Software
BC	Battle Command
C2	Command and Control
C2IPS	Command and Control Information Processing System
C4ISR	Command, Control, Communications, Computers, Intelligence, Surveillance and Reconnaissance
CC	Command and Computers
CCB	Configuration Control Board
CDD	Capability Description Document
CDP	Common Distributed Processing
CDR	Critical Design Review
CHENG	Chief Engineer
CID	Combat Identification
CIS	Combat Intelligence System

CJCSI	Chief Joint Chiefs of Staff Instruction
CJCSM	Chief Joint Chiefs of Staff Memorandum
COE	Common Operating Environment
COTS	Commercial-off-the-Shelf
CP	Computer Program
CPD	Capability Product Description
CTAPS	Contingency Theater Automated Planning System
CTE	Critical Technology Element
DAG	Defense Acquisition Guidebook
DEVNET	Developers Network
DT	Development Testing
DII COE	Defense Information Infrastructure Common Operating Environment
DISA	Defense Information Systems Agency
DoD	Department of Defense
FCS	Future Combat System
FoS	Family of Systems
FTU	Formal Training Unit
GAO	Government Accounting Office
GCSS	Global Command Support System
GFE	Government Furnished Equipment
GIG	Global Information Grid
GOTS	Government-off-the-Shelf
H	Hardware
H/W	Hardware
HMI	Human Machine Interface

IABM	Integrated Architecture Behavioral Model
IAMD	Integrated Air Missile Defense
IBCS	Integrated Air Missile Defense (I) Battle Command System
IEEE	Institute of Electrical and Electronics Engineers, Inc.
IER	Information Exchange Requirement
IETF	The Internet Engineering Task Force
IFC	Integrated Fire Control
INCOSE	The International Council on Systems Engineering
IRL	Integration Readiness Level
IOC	Initial Operating Capability
ISO	International Standards Organization
ISR	Intelligence, Surveillance and Reconnaissance
IT	Information Technologies
JCIDS	Joint Capabilities Integration and Development System
JIIM	Joint, Interagency, Intergovernmental and Multi-National
JV	Joint Vision
KPP	Key Performance Parameter
LISI	Levels of Information Systems Interoperability
LLC	Logical Link Control
LRIP	Low Rate of Production
M	Manufacturing
MAC	Media Access Control
MAIS	Major Automated Information System
MDA	Milestone Decision Authority
MDA	Missile Defense Agency

MDA™	Model Driven Architecture ™
MDAP	Major Defense Acquisition Program
MEI	Major End Item
MS	Milestone
NASA	National Aeronautics and Space Administration
OSI	Open Systems Interconnection
OT&E	Operational Test and Evaluation
OV	Operational View
P	Programmatics
P&F	Plug and Fight
PDR	Preliminary Design Review
PM	Program Manager
QoS	Quality of Service
R&D	Research and Development
RFC	Request for Comments
S	Software
S/W	Software
S&T	Science and Technology
SDD	System Design and Development
SE&I	System Engineering and Integration
SEI	Software Engineering Institute
SFR	System Functional Review
SIAP	Single Integrated Air Picture
SOA	Service Oriented Architecture
SoS	System of Systems

SOSCOE	System of Systems Common Operating Environment
SRL	System Readiness Level
SV	System View
T	Technical
TBMCS	Theater Battle Management Command System
TDS	Technology Development Strategy
TPC	Trusted Partner Certification
TRA	Technology Readiness Assessment
TRL	Technology Readiness Level
TTA	Technology Transition Agreement
TV	Technical View
USD(AT&L)	Under Secretary of Defense for Acquisition, Technology and Logistics
WCCS	Wing Command and Control System
WIN-T	Warfighter Integrated Network – Tactical

THIS PAGE INTENTIONALLY LEFT BLANK

ACKNOWLEDGMENTS

I would like to acknowledge the following people who without their ongoing support this thesis would not have been possible.

I would like to thank Dr. Osmundson for his invaluable lectures, learning activities and feedback on system architecture, system engineering and system-of-systems engineering.

I would like to thank Dr. Mandelbaum and the Institute of Defense Analyses for their generous support, review and guidance of this thesis.

I would like to thank the Office of Naval Research, the Naval Sea Systems Command, and the Single Integrated Air Picture Joint Program Office for their support and commitment to my education. Also, I would like to thank the Department of Navy for providing me the varied and challenging opportunities to learn and excel.

I would like to thank my ever supporting and loving husband and soul mate, Arun Majumdar, for our great life we have together.

I would like to thank my Mom for being my champion and support in all my endeavors whether I was at home, on the other side of the city, across the country or sailing the high seas with the U.S. Navy.

THIS PAGE INTENTIONALLY LEFT BLANK

I. INTRODUCTION

A. PURPOSE

The Chairman of the Joint Chiefs of Staff established the Joint Capabilities Integration and Development System (JCIDS) (Chairman of the Joint Chief of Staff, 2007) processes for acquisition of joint capabilities which are achieved through network-centric applications, services, enterprise systems, Family of Systems (FoS) and System of Systems (SoS). In many cases, advanced technologies must be matured simultaneously by multiple systems to support the degree of interoperability and/or integration required. Current DoD guidance with respect to technology development and assessment is focused on a acquisition of a system which operates relatively independently within a collection of other independent systems.

An approach to technology development and technology readiness assessment of advanced technologies which support network-centric systems is required for successful development and fielding of network centric warfighting capabilities. Fundamental activities of technology maturation and assessments are the definition of a relevant environment and the ability to identify the critical technologies that provide for interoperable or interdependent functions. A review of DoD guidance, industry and academic research shows that there are inconsistent definitions of these network-centric or so called Information Technology (IT) 'systems' and an undefined taxonomy with respect to degrees of interoperability.

This thesis will propose SoS and FoS definitions and an interoperability taxonomy to be used in the context of technology development and assessment of SoS. Given the SoS definitions and a interoperability taxonomy, relevant environment definitions and guidance for identification of critical technologies will be proposed for SoS that would enable the proper technology development and acquisition strategies as well as effective assessment of these technologies. Included will be fundamental requirements and guidelines for SoS Technology Readiness Assessments (TRA) above and beyond the current requirements and guidance for system TRAs.

B. BACKGROUND

The DoD uses advanced technologies to provide for a warfighting edge. Technology maturation is critical to successful development of systems on schedule and within budget while meeting capability requirements. Immature technology drives program schedule, cost, and performance risks at an increasing rate as a system is defined, designed, developed and deployed. The Government Accountability Office (GAO) has reported multiple times on DoD programs that have routinely used advanced technologies that lack the required maturity and led to programs experiencing significant cost overruns and delays.

In the 1990s, the DoD adopted the National Aeronautics and Space Administration's (NASA) Technology Readiness Levels (TRLs) (Mankins, 1995) as an approach to measure technology maturity and established guidance for technology development and assessment consistent with the level of DoD investment at a program acquisition milestone. Initially, NASA's TRLs were primarily defined for hardware. DoD developed and provided guidance for system Technology Readiness Assessments (TRAs) based on these hardware TRLs. Over a five year period, DoD expanded this guidance to include software, manufacturing, and biomedical TRLs. All DoD acquisition programs are required by DoD policy to have technologies matured to a TRL 6 (system/subsystem model or prototype demonstrated in a relevant environment) prior to program initiation at Milestone (MS) B. A successful MS B authorizes a program to enter the System Design and Development (SDD) phase and commits DoD resources to development, production and fielding of a system or capability. This policy was often not enforced. In cases where the technologies were immature, approved technology maturation plans were often required to show how the technologies would be matured. DoD programs continued to experience delays and cost increases due to design and development of the system with immature technologies.

In 2006, Congress passed legislation (United States House of Representatives, 2006) that required the Milestone Decision Authority for Major Defense Acquisition Programs (MDAPs) and Major Automated Information Systems (MAIS) to certify (among other things) that all technologies had reached a TRL 6 with respect to maturity prior to the MS-B. If certification was waived, Congress required the MDAP to provide a justification based on national security needs Also in 2006, The Nunn-McCurdy Act (United States House of Representatives, 2006) which provides for an exception reporting system on DoD MDAP unit costs starting at MS B was revised by the FY06 National Defense Authorization Act (NDAA) to have programs report against the Acquisition Program Baseline (APB) Original Baseline Estimates vice rebaselined estimates for near breach (+15%), significant (+30%) and critical (+50%) cost overruns. These two pieces of legislation make it imperative that a program carefully and thoroughly assess and select mature technologies appropriate to the expected operationally relevant environment to mitigate delays and cost overruns associated with using immature technologies. A network-centric operational environment will be more stressing than that of a system-centric operational environment. Assessment with the current DoD TRA independent system-centric guidance may fall short when used to conduct and certify technology maturity for SoS. It behooves all acquisition programs to manage technology risk appropriately given that at MS-B the APB metrics are put in place that establish maximum thresholds per Nunn-McCurdy for DoD acquisition.

C. DISCUSSION

Technology readiness assessments provide an indication of level of risk to the development of a system and are conducted in support of technology selection, system engineering and program management activities. TRLs are defined levels of maturation from basic science through technology prototyping, development and operational deployment of a system. Two fundamental activities for technology assessment are a definition of the relevant environment and the selection of Critical Technology Elements (CTEs).

> A technology element is 'critical' if the system being acquired depends on this technology element to meet operational requirements with acceptable development cost and schedule and with acceptable production and operational costs and if the technology element of its application is either new or novel (Deputy Under Secretary of Defense for Science and Technology (DUSD(S&T), 2005).

CTEs include software and hardware technologies, algorithms, methods, materials, procedures and techniques. CTEs drive functional and non-functional performance. Examples of non-functional CTEs would be those that are required for test and evaluation, manufacturing, and/or logistics support.

> A relevant environment is a set of stressing conditions representative of the full spectrum of relevant operational employments, which are applied to a CTE as part of a component (TRL 5) or system/subsystem (TRL 6) model or prototype in order to identify whether any design changes or fixes are needed to support the required (threshold) functionality (Mandelbaum, 2007).

The relevant environment for network-centric systems includes the interoperability or integration drivers necessary to a specific warfighting capability. The absence of agreed to definitions of network-centric systems such as enterprise systems, FoS or SoS confounds the ability for technologists to define a relevant environment in which to conducting a technology assessment and the identification of the appropriate CTEs for a capability development.

The Carnegie Melon's Software Engineering Institute (SEI) defines interoperability as:

> the ability of systems, units, or forces to provide services to and accept services from other systems, units, or forces and to use the services exchanged to enable them to operate effectively together (Kasunic and Anderson, 2004).

Note that services are more than just connectivity - there is an implied quality, timeliness, and adherence to specified business processes. SEI's technical note on measuring systems interoperability (Kasunic and Anderson, 2004) defines aspects of technical interoperability (or integration); technical interoperability places detailed demands at multiple levels, which range from physical interconnection to correct interpretation by applications of data provided by other applications. Dimensions of technical interoperability include sensors generating bits of information, communication channels transmitting the bits of information, computers processing the bits of information and weapons directed by messages composed of bits.

> Integration is generally considered to go beyond mere interoperability to involve some degree of functional dependence. For example, a mission planning system might rely on an external intelligence database; an air defense missile system will normally rely on acquisition radar. While interoperable systems can function independently, an integrated system loses significant functionality if the flow of services is interrupted. An integrated family of systems must of necessity be interoperable, but interoperable systems need not be integrated (Kasunic and Anderson, 2004).

There are technical and systemic challenges with a SoS TRA being conducted as a system TRA. Technical challenges include a) Capability requirements and functional analysis should occur prior to specific system requirements, system functional analysis, and system technology development; however, many SoS are assembled from legacy systems and network-centric functionality may be constrained, b) Key Performance Parameters (KPPs) for a capability are not easily allocated to individual systems and their subsystems, c) appropriate SoS relevant environment modeling and simulation and test and evaluation environments will typically be built post system design and development, d) identification of critical technology elements given the interoperability or integration may not be obvious within a (re)composable context or environment and e) SoS are typically enabled with software which is easily changed incrementally over time.

Systemic challenges within the DoD include: a) critical technology developed by the individual programs are in alignment with their respective schedules not the SoS program schedule, b) SoS technology selections and development prior to completion of capability engineering and then individual system(s) engineering drives up risk; SoS engineering needs to be at least through System Functional Review prior to a MS B decision, and c) it's challenging to test the critical technologies in an integrated manner if the individual systems have not had the opportunity to all develop their systems enough to have representative systems for SoS testing (e.g., relevant environment for a integrated heterogeneous distributed system) and d) the fielding of a SoS capability is typically time-phased over several years in capability spirals or increments with differing sets of systems and services.

D. RESEARCH QUESTIONS

The following questions are appropriate when assessing SoS.

1. What are the appropriate definitions of SoS in the context of conducting TRAs?
2. What are the appropriate definitions for interoperability and its use in defining the operational relevant environment for conducting SoS TRAs?
3. What is the approach for determining critical technology elements for SoS?
4. What are the fundamental requirements and guidelines for conducting a SoS TRA and how are these different from a system TRA?
5. What technology development and acquisition strategies should be employed for technology maturation for SoS given the challenges of synchronization of individual system acquisition schedules?
6. When is the ‘right’ time to hold SoS acquisition milestones given the synchronization issues with the individual systems that make up the SoS?

E. BENEFIT OF STUDY

This study will benefit Science and Technology (S&T), Acquisition professionals and Senior Executives in the DoD in the conduct of TRAs in support of SoS acquisition.

F. SCOPE

The thesis will focus on SoS TRAs. SoS definitions, an interoperability taxonomy and relevant SoS environment definitions and guidance for identification of critical technologies will be proposed that will enable the proper technology development and acquisition strategies will be defined. This thesis will recommend additional requirements and guidelines for SoS TRAs above and beyond the current requirements and guidance for system TRAs.

This thesis is scoped to address technology maturity only. A distinction is made in this thesis between technology maturity and a technology’s readiness to be transitioned (transitionability). Technology maturity is defined as the technology’s state or condition with respect to full/complete development as required to be emplaced in a system and provide for a specified functionality and performance. Maturity can not be used as the only selection criteria for technology; technology needs to be assessed in the context of the total capability development over time and the acquisition strategy of said capability.

Technology maturity is by definition considered as one aspect of technology's readiness to be transitioned. Technology transitionability is measured as a function of the technology's maturity, availability (program has access to the technology), alignment of technology and program schedules, and sufficiency of funding to develop/modify/insert programmatically into the system.

G. METHODOLOGY

Qualitative methods are used in this thesis. Content analysis and participant observation are performed on DoD and DoD industry, non-DoD industry, and academic sources regarding system and SoS acquisition, interoperability and Integration, TRAs, and system and SoS engineering. Analysis of successful and failing SoS acquisitions is performed to determine how technology readiness assessments supported or failed to support their acquisition. These materials are synthesized into a concise articulation of requirements and guidance for SoS TRAs.

H. ORGANIZATION OF STUDY

The plan of this thesis is as follows: Chapter II provides an overview of literature on the topic of technology readiness assessments as well as related literature on SoS and interoperability, Chapter III synthesizes the literature review, Chapter IV provides preliminary analysis for SoS TRAs, and finally, Chapter V gives the summary, conclusions and recommendations for future actions and research regarding SoS TRAs.

THIS PAGE INTENTIONALLY LEFT BLANK

II. LITERATURE REVIEW

A. APPROACH

This literature review encompasses system(s) definitions, interoperability definitions, selected ‘system’ examples and an overview of technology readiness assessments. Sources include books, articles, reports, and briefings from government, industry and academia sources. This literature review supports the content analysis research method for this SoS TRA topic. A SoS definition will be explored as a foundation for SoS technology readiness assessment. Interoperability will be explored to assist in identification and types of CTEs. Finally, technology readiness assessments will be analyzed within a view towards SoS TRAs. The following content analysis questions are answered at the beginning of each section:

1. What data was analyzed?
2. Why was this data identified to by analyzed?
3. What is the domain from which it was drawn – DoD/government, non-DoD industry or academia?
4. What is the context relative to which the data are analyzed?
5. What are the boundaries of the analysis?
6. What is the target of the inferences?

B. SYSTEMS

There are a variety of ‘systems’ from subsystems, systems, family of systems, system of systems, and enterprise systems. Network-centric systems require the connection of systems and may lead to some sense of unboundedness. The first step to defining a system is to delineate the boundary. The DoD requirements process and the nature of joint warfare for a specific mission area or task drives the scope of system connections. Without defining clearly the boundary of a system and what is to be developed, evaluated and deployed there may be less performance in a network-centric force than that of a system-centric one.

Concise definitions of SoS type are useful in identifying critical functions and the technologies required to enable these functions. The scope of the operationally relevant environment is constrained by the scope of the boundary at which to measure performance with respect to specified KPPs. The boundary of SoS is proposed to be encompassing a number of systems; therefore, architectural artifacts will be reviewed.

A review of the DoD, industry, and academic literature finds multiple definitions for SoS or IT systems. Given a definition of the degree of interoperability, these SoS definitions may become clear. This literature review will review the tasks and/or missions the systems provide for and the degree of interoperability required to support defining SoS and the types of SoS if appropriate.

DoD related literature is useful given the context of joint warfighting. Academic research is focused toward advanced concepts and technologies which may be applied in the future, whereas, commercial industry will provide the perspective of ubiquitous and diverse systems of all types (e.g., financial, medical) being developed and used globally.

1. System of Systems Government/DoD Industry Literature Summary

Prior to defining SoS, one needs to define system given at some level the SoS is a 'system'. In reviewing DoD literature there were numerous and varying definitions for 'system'. DoD-STD 480A defines system as follows:

> A composite of subsystems, assemblies (or sets), skills, and techniques capable of performing and/ or supporting an operational (or nonoperational) role.

The JCIDS is governed by the Chairman of the Joint Chiefs of Staff Instruction, CJCSI 3170.01F, latest dated 1 May 2007. This instruction defines:

> Joint concepts-centric capabilities identification process that will allow joint forces to meet the full range of military operations and challenges of the future. Meeting these challenges involves a transformation to a fully integrated, expeditionary, networked, decentralized, adaptable and lethal joint force able to achieve decision superiority…Potential solutions may include a family of systems (FoS) that take different approaches to filling the capability gap, each addressing operational considerations in a different way. Alternatively, the solution may require a system of systems (SoS) approach to fill a capability gap. The FoS and SoS materiel solutions may also require systems delivered by multiple sponsors and materiel developers…Capability Description Documents (CDDs) and Capability Production Documents (CPDs) developed in accordance with this instruction will be accepted to support capability development.

A CDD may not define the allocation of KPPs to individual systems. Capability is defined as “the ability to achieve a desired effect under specified standards and conditions through combinations of means and ways to perform a set of tasks.’ See Figure 1 for a perspective on capability-based system engineering.

The CJCSI 3170 defines:

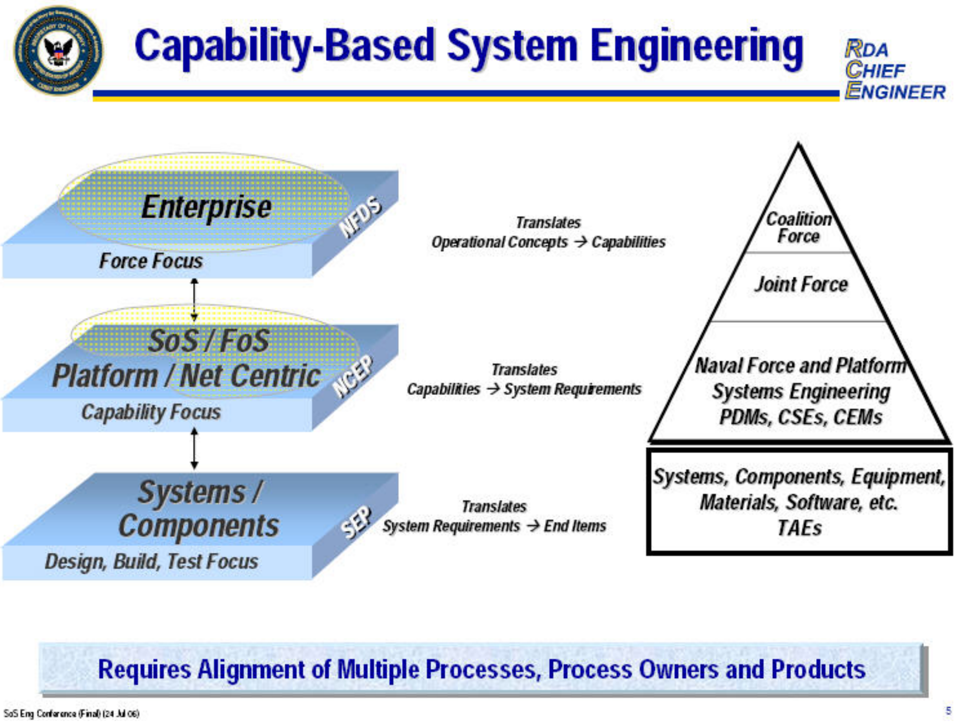
> Family of Systems – A set of systems that provide similar capabilities through different approaches to achieve similar or complementary effects. For instance, the warfighter may need the capability to track moving targets. The FoS that provides this capability could include unmanned or manned aerial vehicles with appropriate sensors, a space-based sensor platform or a special operations capability. Each can provide the ability to track moving targets, but with differing characteristics of persistence, accuracy, timeliness, etc.

The CJCSI 3170 defines:

> Net centric – Relating to or representing the attributes of net-centricity. Net-centricity is a robust, globally interconnected network environment (including infrastructure, systems, processes and people) in which data is shared timely and seamlessly among users, applications and platforms.

The CJCSI 3170 defines:

> System of Systems – A set or arrangement of interdependent systems that are related or connected to provide a given capability. The loss of any part of the system will significantly degrade the performance or capabilities of the whole. The development of a SoS solution will involve trade space between the systems as well as within an individual system performance.



Capability-Based System Engineering

RDA
CHIEF
ENGINEER

Enterprise
Force Focus
NFDS

SoS / FoS
Platform / Net Centric
Capability Focus
NCEP

Systems /
Components
Design, Build, Test Focus
SEP

Translates
Operational Concepts → Capabilities

Translates
Capabilities → System Requirements

Translates
System Requirements → End Items

Coalition Force

Joint Force

Naval Force and Platform
Systems Engineering
PDMs, CSEs, CEMs

Systems, Components, Equipment,
Materials, Software, etc.
TAEs

Requires Alignment of Multiple Processes, Process Owners and Products

SoS Eng Conference (Final) (24 Jul 06)

5

Figure 1. Capability-Based System Engineering [From: Siel, 2006]

Given the above definitions, one may come to the conclusion that it holds true only for a system of systems that if one system fails that the whole degrades. This may or may not be true given the robustness of the number of systems in the SoS. In fact, one may consider that for a minimized FoS that degradation may be as likely to occur where each ‘family’ member has a complementary mission to do that none of the family member have a capability to perform as well.

From the DoD Guidebook (Under Secretary of Defense for Acquisition, Technology and Logistics (USD(AT&L), 2006) Chapter 4.2.6 on Systems Engineering:

> A family of systems does not create capability beyond the additive sum of the individual capabilities of its member systems. A family of systems is basically a grouping of systems having some common characteristic(s). For example, each system in a family of systems may belong to a domain or product lines (e.g., a family of missiles or aircraft). A family of systems lacks the synergy of a system of systems. The family of systems does not acquire qualitatively new properties as a result of the grouping. In fact, the member systems may not be connected into a whole.

From the DoD Acquisition Guidebook (DAG) (USD(AT&L), 2006) Chapter 4.2.6 on Systems Engineering- this definition is the same at the definition in the CJCSI 3170:

> A system of systems is a set or arrangement of interdependent systems that are related or connected to provide a given capability. The loss of any part of the system will significantly degrade the performance or capabilities of the whole. The development of a system of systems solution will involve trade space between the systems as well as within an individual system's performance.

DoD has a draft Systems of Systems (SoS) Systems Engineering Guide: Considerations for Systems Engineering in a System of Systems Environment, version .9 dated Dec 22, 2006 (USD(AT&L), 2006). It provides for extensions of traditional system engineering processes; however, it doesn't distinguish between SoS and FoS. The guide defines a system as 'an integrated composite of people, products, and processes that provide a capability to satisfy a stated need or objective' and 'a capability is the ability to achieve a desired effect under specified standards and conditions through combinations of ways and means to perform a set of tasks (citing CJCSM 3170.01B, May 11, 2005 – note: no change in the 01 May 07 version).' It then defines SoS as:

> a set or arrangement of systems that results when independent and useful systems are integrated into a larger system that delivers unique capabilities (USD(AT&L), 2006). When integrated, the independent systems can become interdependent, which is a relationship of mutual dependence and benefit between the integrated systems. Both systems and SoS conform to the accepted definition of a system in that each consists of parts, relationships, and a whole that is greater than the sum of the parts; however, although an SoS is a system, not all systems are SoS.

The guide states:

> For the SoS to function, its constituent systems must be integrated to achieve not only physical connectivity, but interoperability at all levels, including physical, logical, semantic, and syntactic interoperability. Interoperability allows the necessary connectivity across the SoS to be defined.

The guide goes on to state:

> The boundary of any SoS can be relatively ambiguous because of the dynamic operational focus, multi-mission, and often ad hoc nature of the operational environment of the SoS. In this type of environment, there is a potential for ad hoc coupling across both organizational and systems

> boundaries in support of the dependencies created. Therefore, in order to use systems successfully, in a SoS context, the protocols used to support the specification of interfaces should be ubiquitous because they are key convergence points for SoS and there may be no opportunity for changes to the interfaces without major impact to the entire SoS. The development and management of a SoS architecture through the evolution of an SoS is the mechanism used to document and share information among constituent systems to support integration.

2. Non-DoD Industry Literature Summary

The Institute of Electrical and Electronics Engineers, Inc. (IEEE)'s definition of system is:

> a set of functional elements organized to satisfy user needs (IEEE, 1994)" and/or "a collection of components organized to accomplish a specific function or set of functions (IEEE, 2002)

Commercial industry literature including the International Council on System Engineering (INCOSE) has comparatively very little written about SoS and FoS from any organizations other than DoD and DoD Industry.

In industry family of systems refers to a system that has several 'variants' that a similar to each other. They are not necessarily ever connected to work together.

3. Academia Literature Summary

Maier and Rechtin defines a system as:

> a collection of things or elements which, working together, produce a result not achievable by the things alone (Maier and Rechtin, 2002).

A system of systems is described by Maier and Rechtin as systems which are operationally independent, managerially independent, evolutionary developed, with emergent behavior and are geographically distributed. The following definitions apply (Maier and Rechtin, 2002):

Operational Independence of the Elements: If the SoS is disassembled into its component systems the component systems must be able to usefully operate independently. The SoS is composed of systems which are independent and useful in their own right.

Managerial Independence of the Elements: The component systems not only can operate independently, they do operate independently. The component systems are separately acquired and integrated but maintain a continuing operational existence independent of the SoS.

Evolutionary Development: The SoS does not appear fully formed. Its development and existence is evolutionary with functions and purposes added, removed, and modified with experience.

Emergent Behavior: The system performs functions and carries out purposes that do not reside in any component system. These behaviors are emergent properties of the entire SoS and cannot be localized to any component system. The principal purposes of the SoS are fulfilled by these behaviors.

Geographic Distribution: The geographic extent of the component systems is large. Large is a nebulous and relative concept as communication capabilities increase, but at a minimum it means that the components can readily exchange only information and not substantial quantities of mass or energy.

Maier and Rechtin goes on to describe three different types of SoS, Virtual, Voluntary, and Directed, and states not all SoS of similar complexity and extent should be regarded as equivalent. An additional dimension, that of managerial control, is stated as critical to identifying the types of SoS. The three basic SoS driven by managerial control as defined by Maier and Rechtin are as follows (Maier and Rechtin, 2002):

Directed: Directed systems are those in which the integrated SoS is built and managed to fulfill specific purposes. It is centrally managed during long term operation to continue to fulfill those purposes, and any new ones the system owners may wish to address. The component systems maintain an ability to operate independently, but their normal operational mode is subordinated to the central managed purpose. For example, an integrated air defense network is usually centrally managed to defend a region against enemy systems, although its component systems may operate independently.

Collaborative: Collaborative systems are distinct from directed systems in that the central management organization does not have coercive power to run the system.

The component systems must, more or less, voluntarily collaborate to fulfill the agreed upon central purposes. The Internet is a collaborative system. The IETF works out standards, but has no power to enforce them. Agreements among the central players on service provision and rejection provide what enforcement mechanism there is to maintain standards. The Internet began as a directed system, controlled by the Advanced Research Projects Agency, to share computer resources. Over time it has evolved from central control through unplanned collaborative mechanisms.

Virtual: Virtual systems lack a central management authority. Indeed, they lack a centrally agreed upon purpose for the SoS. Large scale behavior emerges, and may be desirable, but the supersystem must rely upon relatively invisible mechanisms to maintain it. A virtual system may be deliberate or accidental. Familiar examples of what is called here a virtual system are the World Wide Web and national economies. Both 'systems' are distributed physically and managerially. The World Wide Web is even more distributed than the Internet in that no agency ever exerted real central control. Control has been exerted only through the publication of standards for resource naming, navigation, and document structure. Web sites choose to obey the standards or not at their own discretion. The system is controlled by the forces that make cooperation and compliance to the core standards. The standards do not evolve in a controlled way; rather they emerge from the market success of various innovators. National economies and the social 'systems' that surround us might be thought of as virtual systems. Politicians regularly try to architect these systems, sometimes through forceful means, but the long-term nature is determined by highly distributed, partially invisible mechanisms.

Dr's. Boardman and Sauser (Boardman and Sauser, 2006) describe differentiating characteristics of a SoS as:

> autonomy exercised by the constituent systems in order to fulfill the purpose of the SoS, constituent systems choose to belong to the SoS for greater good, SoS are typically connected dynamically to enhance the SoS performance, and characterized by a diversity of systems.

Also of concern, SoS may seem unbounded. The levels of connectivity, platform diversity and degree of associated interoperability points to the risk of whether the SoS is unbounded. Bounded systems are characterized by centralized data and control, systems and their linkages are known a priori and are specific to the connection and interoperability specified. Unbounded systems are characterized by protocols which provide a loose coupling and are omnipresent and allow for dynamic spontaneous connections (DiMario, 2006).

Most SoS literature focuses on enabling interoperability via integration and therefore, focuses on architecture first. Remembering that interoperability is concerned with connectivity, capacity, correctness, accuracy, bandwidth, data latency, syntactic compatibility, consistency, completeness and undesirable semantic emergent behavior as cited above, we look at the architecture products developed during system engineering activities.

Systems engineering methods provide a basis for exploring system interoperability. Figure 2 shows the Operational, System, and Technical architecture related views and their relationships that get created during the system engineering processes (Habayeb, 2005).

Concept of operations within the context of an existing or to-be Enterprise architecture and mission requirements provide constraints and restraints on architecture, system development, and degrees of interoperability. The operational view provides for information exchanges, types of interoperability, and KPPs required to support a mission. The systems view defines system attributes, and provides the basis for comparing system performance against operational requirements. The technical view defines the standards and protocols to be implemented by the system for interoperability.

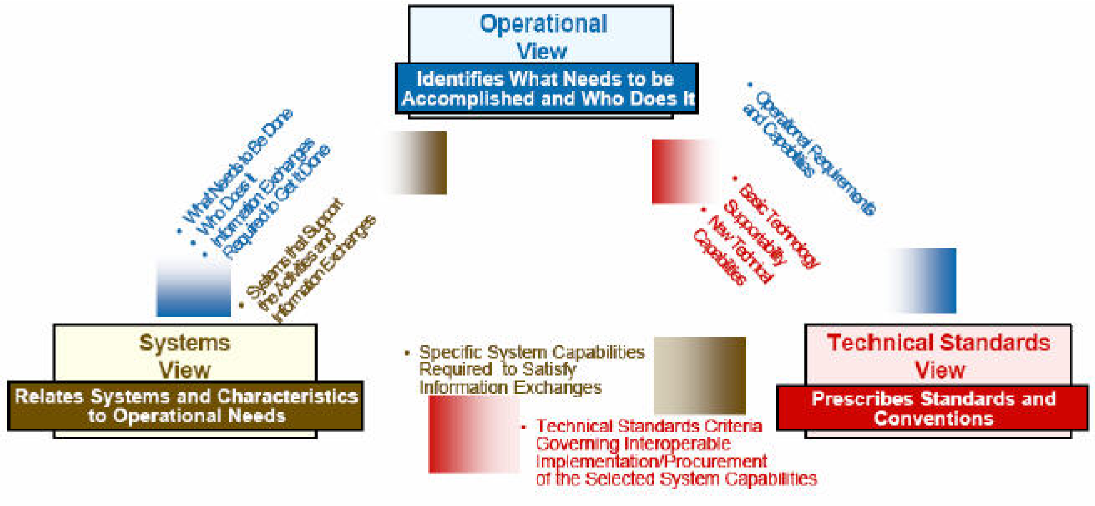

Operational View
Identifies What Needs to be Accomplished and Who Does It
• What Needs to Be Done
• Who Does It
• Information Exchanges Required to Get It Done
• Systems that Support the Activities and Information Exchanges
• Operational Requirements and Capabilities
• Basic Technology Supportability
• New Technical Capabilities
Systems View
Relates Systems and Characteristics to Operational Needs
• Specific System Capabilities Required to Satisfy Information Exchanges
• Technical Standards Criteria Governing Interoperable Implementation/Procurement of the Selected System Capabilities
Technical Standards View
Prescribes Standards and Conventions

Figure 2. Linkages Among Architectural Views [From: Habayeb, 2005]

Taking a deeper look into the Operational Views (OV) artifacts (see Figure 3):

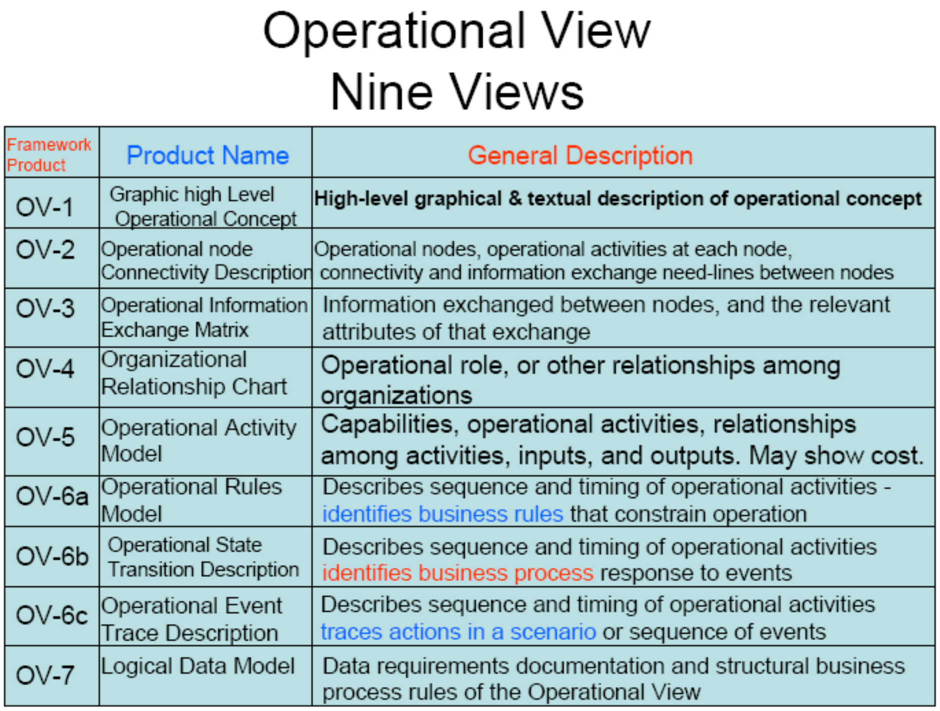
- The OV-1 provide a description of the operational concept
- The OV-2 identifies the operational nodes, operational activities at each node, and the information exchanges needed between nodes.
- The OV-3 identifies the information exchanges between nodes
- The OV-5 identifies capabilities, relationships among activities and inputs and outputs.
- The OV-6 describes the sequencing and timing of activities as well as business rules and processes.
- The OV-7 documents the data requirements and business rules.

System views (as seen in Figures 4 and 5) provide the detailed information regarding functionality required and the interfaces needed to enable this functionality. Taking a deeper look into the System Views (SV) one finds:

- The SV-1 identifies the system nodes and interconnections between the nodes.
- The SV-2 defines the communications architecture.
- The SV-3 describes the interfaces.
- The SV-4 documents the system functions and the data flow between them.
- The SV-5 maps functions and operational activities
- The SV-6 documents the data element exchanges

- The SV-7 documents the performance characteristics including the timelines.
- The SV-11 documents the physical implementation e.g., messages

The Technical Views (TV), TV-1 and TV-2 are used to represent current and future standards.

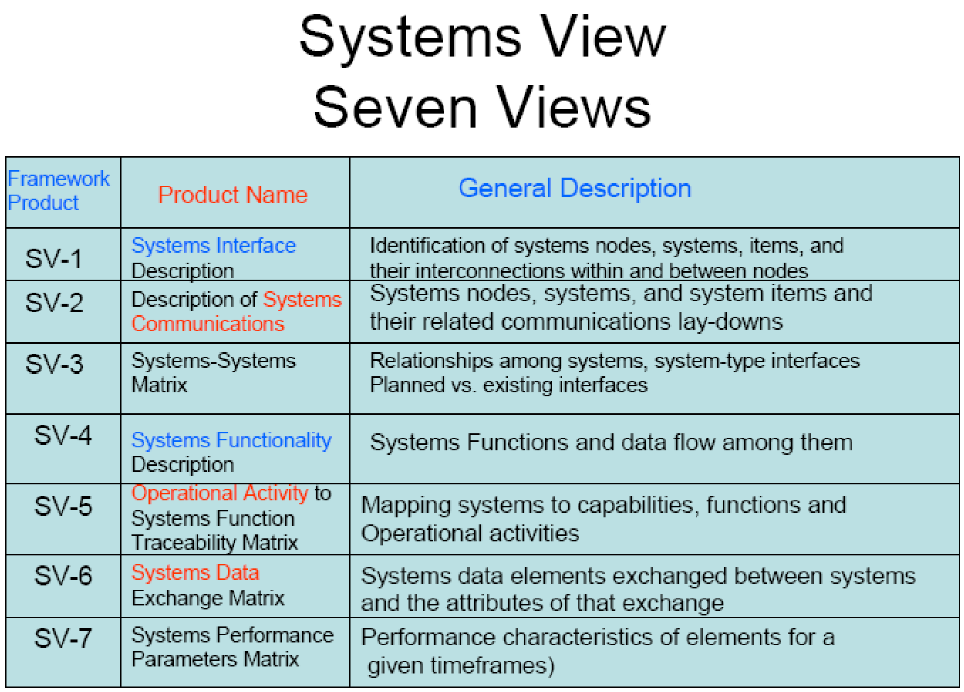


Operational View
Nine Views

Framework Product	Product Name	General Description
OV-1	Graphic high Level Operational Concept	**High-level graphical & textual description of operational concept**
OV-2	Operational node Connectivity Description	Operational nodes, operational activities at each node, connectivity and information exchange need-lines between nodes
OV-3	Operational Information Exchange Matrix	Information exchanged between nodes, and the relevant attributes of that exchange
OV-4	Organizational Relationship Chart	Operational role, or other relationships among organizations
OV-5	Operational Activity Model	Capabilities, operational activities, relationships among activities, inputs, and outputs. May show cost.
OV-6a	Operational Rules Model	Describes sequence and timing of operational activities - identifies business rules that constrain operation
OV-6b	Operational State Transition Description	Describes sequence and timing of operational activities identifies business process response to events
OV-6c	Operational Event Trace Description	Describes sequence and timing of operational activities traces actions in a scenario or sequence of events
OV-7	Logical Data Model	Data requirements documentation and structural business process rules of the Operational View

Figure 3. Operational Views OV-1 to OV-9 [From: Habayeb, 2005]

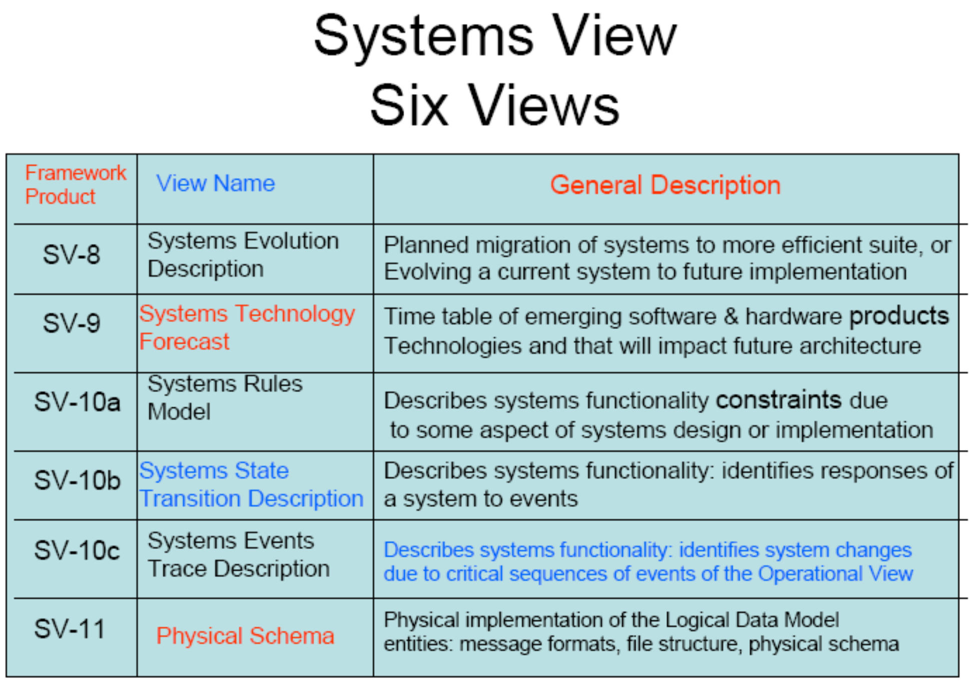
It's useful to now look (see Figure 6) at these architectural views and translate them into system engineering views to facilitate looking at inputs and outputs and their timing from an operational view, looking at data flows and logic at a system functional view, and looking at the physical interfaces that will enable to required operational requirements and system functions.



Systems View
Seven Views

Framework Product	Product Name	General Description
SV-1	Systems Interface Description	Identification of systems nodes, systems, items, and their interconnections within and between nodes
SV-2	Description of Systems Communications	Systems nodes, systems, and system items and their related communications lay-downs
SV-3	Systems-Systems Matrix	Relationships among systems, system-type interfaces Planned vs. existing interfaces
SV-4	Systems Functionality Description	Systems Functions and data flow among them
SV-5	Operational Activity to Systems Function Traceability Matrix	Mapping systems to capabilities, functions and Operational activities
SV-6	Systems Data Exchange Matrix	Systems data elements exchanged between systems and the attributes of that exchange
SV-7	Systems Performance Parameters Matrix	Performance characteristics of elements for a given timeframes)

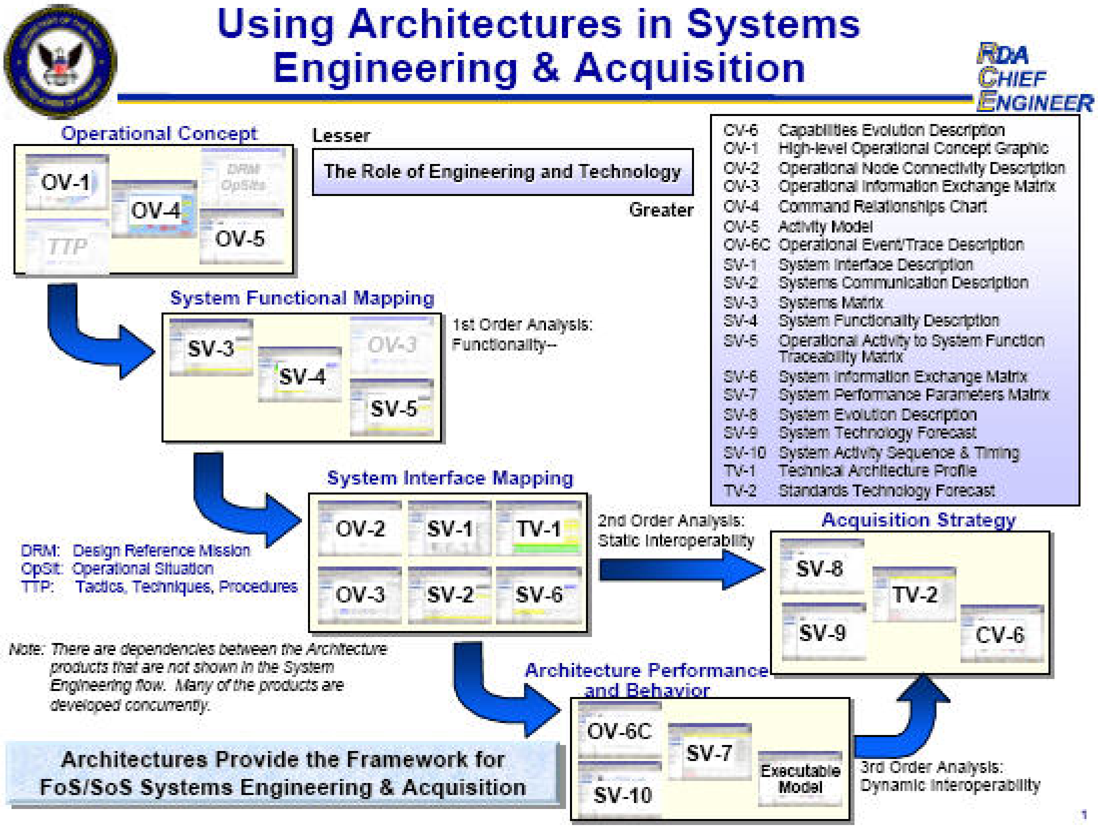
Figure 4. System Views one through seven [From: Habayeb, 2005]



Systems View
Six Views

Framework Product	View Name	General Description
SV-8	Systems Evolution Description	Planned migration of systems to more efficient suite, or Evolving a current system to future implementation
SV-9	Systems Technology Forecast	Time table of emerging software & hardware **products** Technologies and that will impact future architecture
SV-10a	Systems Rules Model	Describes systems functionality **constraints** due to some aspect of systems design or implementation
SV-10b	Systems State Transition Description	Describes systems functionality: identifies responses of a system to events
SV-10c	Systems Events Trace Description	Describes systems functionality: identifies system changes due to critical sequences of events of the Operational View
SV-11	Physical Schema	Physical implementation of the Logical Data Model entities: message formats, file structure, physical schema

Figure 5. System Views eight through eleven [From: Habayeb, 2005]



Using Architectures in Systems Engineering & Acquisition

RDA CHIEF ENGINEER

CV-6	Capabilities Evolution Description
OV-1	High-level Operational Concept Graphic
OV-2	Operational Node Connectivity Description
OV-3	Operational Information Exchange Matrix
OV-4	Command Relationships Chart
OV-5	Activity Model
OV-6C	Operational Event/Trace Description
SV-1	System Interface Description
SV-2	Systems Communication Description
SV-3	Systems Matrix
SV-4	System Functionality Description
SV-5	Operational Activity to System Function Traceability Matrix
SV-6	System Information Exchange Matrix
SV-7	System Performance Parameters Matrix
SV-8	System Evolution Description
SV-9	System Technology Forecast
SV-10	System Activity Sequence & Timing
TV-1	Technical Architecture Profile
TV-2	Standards Technology Forecast

DRM:	Design Reference Mission
OpSit:	Operational Situation
TTP:	Tactics, Techniques, Procedures

Note: There are dependencies between the Architecture products that are not shown in the System Engineering flow. Many of the products are developed concurrently.

Architectures Provide the Framework for FoS/SoS Systems Engineering & Acquisition

1

Figure 6. Using Architecture in System Engineering [From: Dickerson and Soules, 2002]

Interoperability and integration are implemented by interfaces between systems and subsystems. Interfaces provide for functional and physical integration to enable an operational capability and as such are critical parts of a system or SoS. Functional and physical interfaces drive architecture. A careful analysis of the architecture and system engineering views will identify where critical technologies will exist.

4. DoD System of Systems and Family of Systems Examples

DoD is currently developing a number of SoSs and FoSs. A selection of four legacy, new and mixed FoS and SoSs are reviewed to provide a diversity of SoS and FoS perspectives.

a. Army's Future Combat System

The Army is reorganizing its current forces into modular brigade combat teams. The Future Force is designed to be a deployable and responsive force and enables the Army to move away from the large division-centric structure of the past. Each brigade combat team is expected to be highly survivable and the most lethal brigade-sized unit the Army has ever fielded. The Army's Future Combat Systems (FCS) is the answer to this need and the FCS family of weapons (systems) includes 18 types of manned and unmanned ground vehicles, air vehicles, sensors, and munitions linked by a information network plus the soldier (note: first deployment of FCS is now 14 plus a network and the soldier). The network allows the FCS Family-of-Systems (FoS) to operate as a cohesive SoS where the whole of its capabilities is greater than the sum of its parts (Future Combat System Program Office, 2007). See Figure 8 for the Operation View -1 of FCS.

FCS has a SoS Common Operating Environment (SOSCOE) central to the implementation of the FCS network, which supports multiple mission-critical applications independently and simultaneously. It is configurable so that any specific instantiation can incorporate only the components that are needed for that instantiation. SOSCOE enables straightforward integration of separate software packages, independent of their location, connectivity mechanism and the technology used to develop them.

b. DoD's Global Combat Support System

DoD's Global Combat Support System (GCSS) FoS includes a mix of systems that can be tailored to provide focused logistics capabilities. The GCSS FoS consists of Service and Defense Agency authoritative single, end-to-end capability enabled by information systems from which actionable, real time, accurate data can be accessed to manage and monitor units, personnel and equipment through all stages of the mobilization process. It is developed and maintained with standard core information technology services and capabilities required across the FoS including the Defense Information Infrastructure Common Operating Environment (DII COE). GCSS has developed a trusted partner certification (TPC) relationship with developers, contractors and government agencies for rapid acceptance and distribution of software patches and upgrades in order to maintain the GCSS FOS as current, useful, and up to date on a worldwide basis (Joint Chiefs of Staff, 2002). The DII COE is a framework for the construction of modular, scalable, distributed Command, Control, Computer, Communications, Intelligence, Surveillance and Reconnaissance (C4ISR) computer systems. It is a collection of tools for the creation of these systems; it is a set of software modules that can be (re-)used to construct these systems (Frazier, 2001) DII COE includes a kernel (operating system, security, and software install tools, infrastructure services (data exchange, network management, communications) and common support applications (e.g., alerts, messaging).

The GCSS FoS consists of the following systems and their components:

(1) GCSS Air Force

(2) GCSS Army

(3) GCSS Marine Corps

(4) Navy GCSS capabilities/GCSS maritime

(5) Global Transportation Network 21

(6) Joint Total Asset Visibility/DLA Business System Modernization

(7) Defense Integrated Military Human Resources System

(8) Theater Medical Information Program

(9) Defense Information Systems Agency's (DISA) GCSS (combatant commander/JTF)

(10) Defense Finance and Accounting System Integrated Data Environment

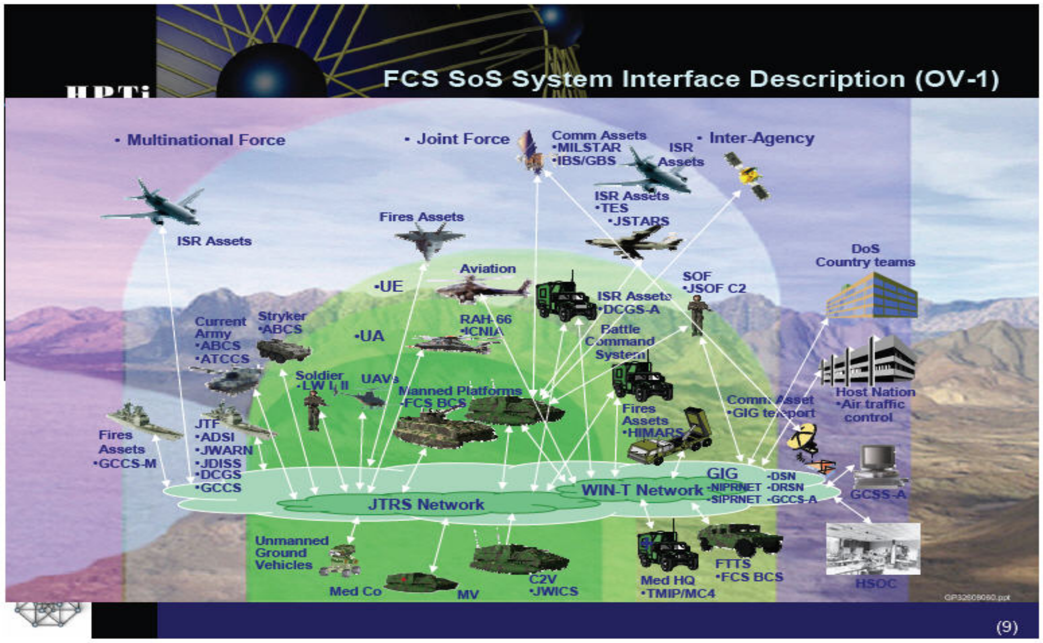
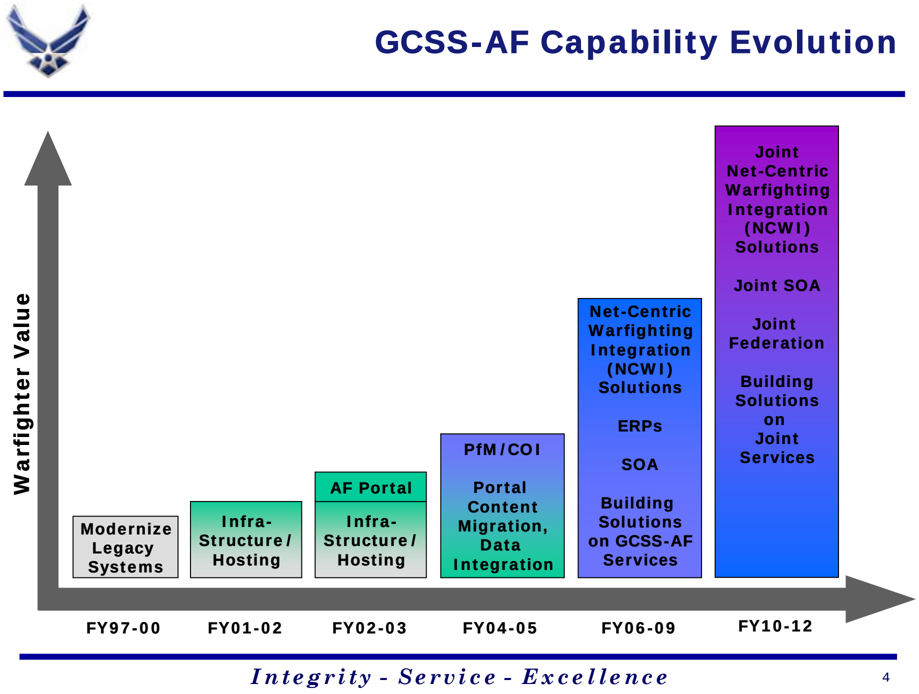


Figure 7. Future Combat System OV-1 [From: Powell, 2006]

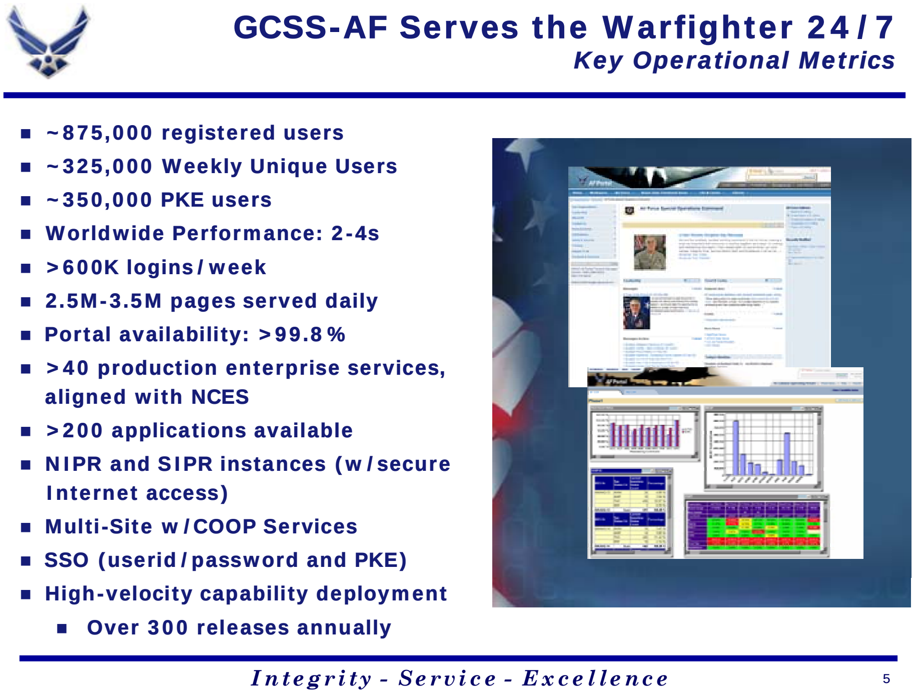
GCSS Air Force has grown to encompass IT Enterprise Services via Service Oriented Architecture approach. See Figure 9 and 10. The Army and Marine Corps systems have stayed with a focus on warfighting logistics support.


GCSS-AF Capability Evolution

Integrity - Service - Excellence 4

Figure 8. GCSS-AF Capability Evolution [From: GCCS-AF Team, 2006]

The Air Force's Theater Battle Management Command System (TBMCS) is the set of application tools used by the Joint Forces Air Component Commander (JFACC) to plan and execute theater air operations. The TBMCS is the umbrella program for the various systems in an Air Operational Control (AOC) Center. TBMCS purpose is to provide a set of connected applications to collect, process and distribute data to support employment of air power. This includes the Contingency Theater Automated Planning System (CTAPS), Combat Intelligence System (CIS), Wing Command and Control System (WCCS), and the Command and Control Information Processing System (C2IPS) software applications. It has been deployed in spirals and with each spiral has moved towards an Enterprise system giving operators real-time access to the status of air operations across the theater via the web.



GCSS-AF Serves the Warfighter 24/7

Key Operational Metrics

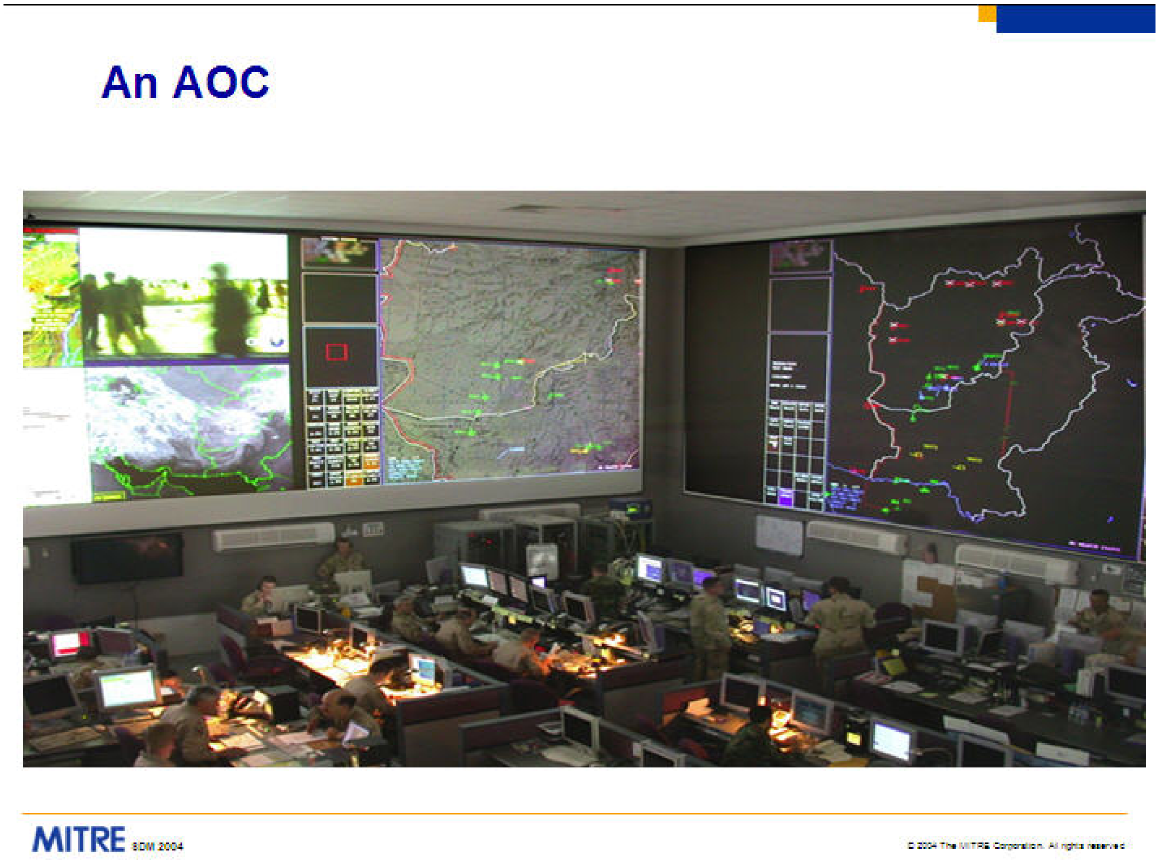
- ~875,000 registered users
- ~325,000 Weekly Unique Users
- ~350,000 PKE users
- Worldwide Performance: 2-4s
- >600K logins/week
- 2.5M-3.5M pages served daily
- Portal availability: >99.8%
- >40 production enterprise services, aligned with NCES
- >200 applications available
- NIPR and SIPR instances (w/secure Internet access)
- Multi-Site w/COOP Services
- SSO (userid/password and PKE)
- High-velocity capability deployment
  - Over 300 releases annually

Integrity - Service - Excellence 5

Figure 9. GCSS Key Operational Metrics [From: GCCS-AF Team, 2006]

c. *Air Force's Theater Battle Management Command System*

The AOC was known as a 'System of Systems' (SoS). As such, it was envisioned as a system assembled of other systems so as to offer the capabilities needed to perform roles assigned to an AOC. Implicit in this was the expectation that the systems from which the AOC was assembled could be composed into an AOC SoS. The AOC today is assembled from 80+ applications and systems. There are infrastructure elements, communication elements, applications, servers, and databases. The goal was to compose the desired capabilities from the elements found in, or which could be brought into, the AOC (See Figure 11) (Norman and Kuras, 2004).



An AOC

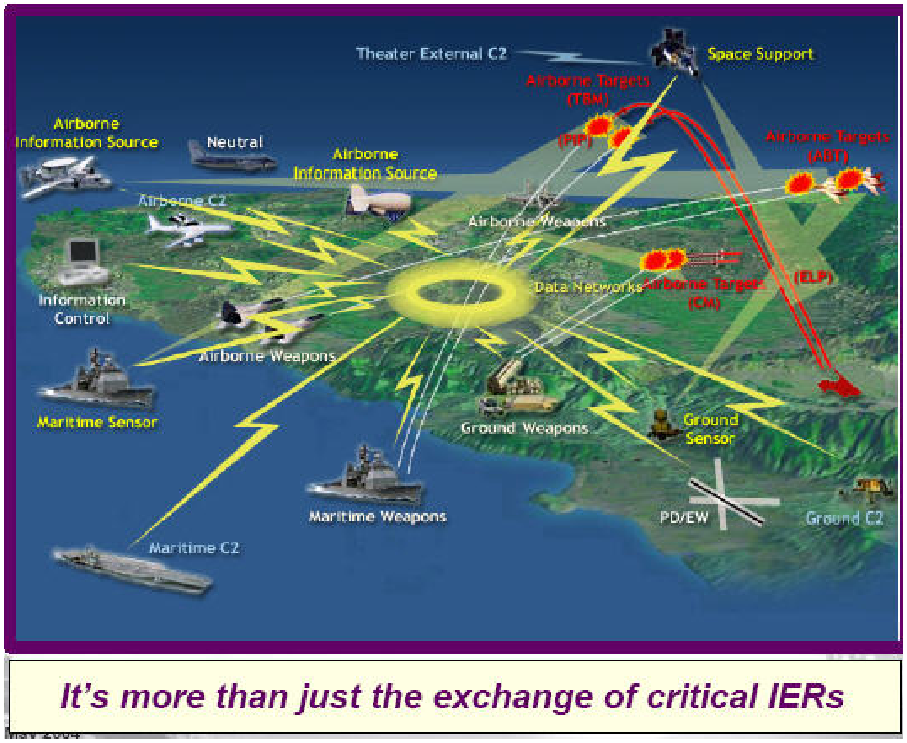
MITRE SDM 2004

© 2004 The MITRE Corporation. All rights reserved

Figure 10. Air Operations Center (AOC) [From: Norman and Kuras, 2004]

d. *DoD Single Integrated Air Picture System of Systems and Army's Integrated Air Missile Defense System of Systems*

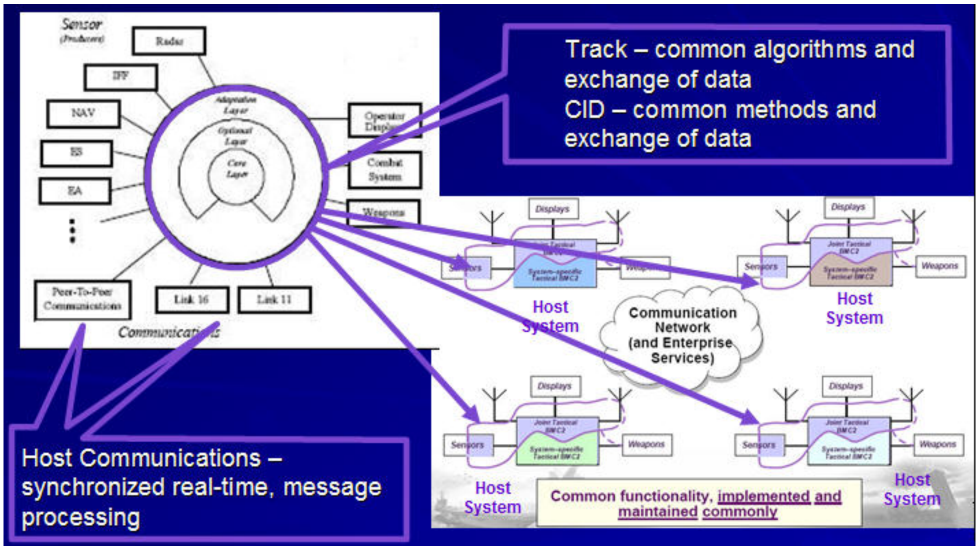
DoD has embarked on developing a SoS a Single Integrated Air Picture (SIAP) (see OV-1 in Figure 12). SIAP is built via an Integrated Architecture Behavioral Model (IABM) which when instantiated in a combat system provides for distributed common processing of data/information (see Figure 13). SIAP is an enabling capability for mission capabilities such as missile defense. The IABM is built using a Model Driven Architecture™ approach. Its goal is a fused, common, continuous, unambiguous track of all airborne objects with one, and only one, track number. The SIAP will fuse near-real-time and real-time data allowing users to have identical information about each detected airborne object. MDA™ allows developers to focus on specifying platform independent business logic and automates the translation of that business logic to target programming language, operating system, middleware, database or other information technology specifics.



It's more than just the exchange of critical IERs

Figure 11. Single Integrated Air Picture OV-1 [From: Wilson, 2004]

The Army's Integrated Air Missile Defense (IAMD) System of System includes SIAP in addition to its missile defense capabilities (see Figure 14). IAMD SoS enables a larger defended area against a number of different types of threats while providing for flexibility in type of interceptors or other types of weapons. IAMD is accomplished via a Common IAMD Battle Command System (IBCS) and plug and fight modules at each of the sense, control, engage nodes. The SIAP IABM is part of the plug and fight modules. The Army adds service specific common functionality to the plug and fight modules. This SoS shows how one SoS can be part of another SoS without overlapping of systems - one SoS is not inside other; SIAP SoS is not contained in IAMD SoS. The FCS SOSCOE is to be used with the IAMD SoS in a future spiral. If this does happen there will be an IAMD SoS using a FCS SOSCOE with the SIAP SoS IABM.


Track – common algorithms and exchange of data
CID – common methods and exchange of data

Host Communications – synchronized real-time, message processing

Common functionality, implemented and maintained commonly

Figure 12. Integrated Architecture Behavior Model [After Ref Wilson, 2004]

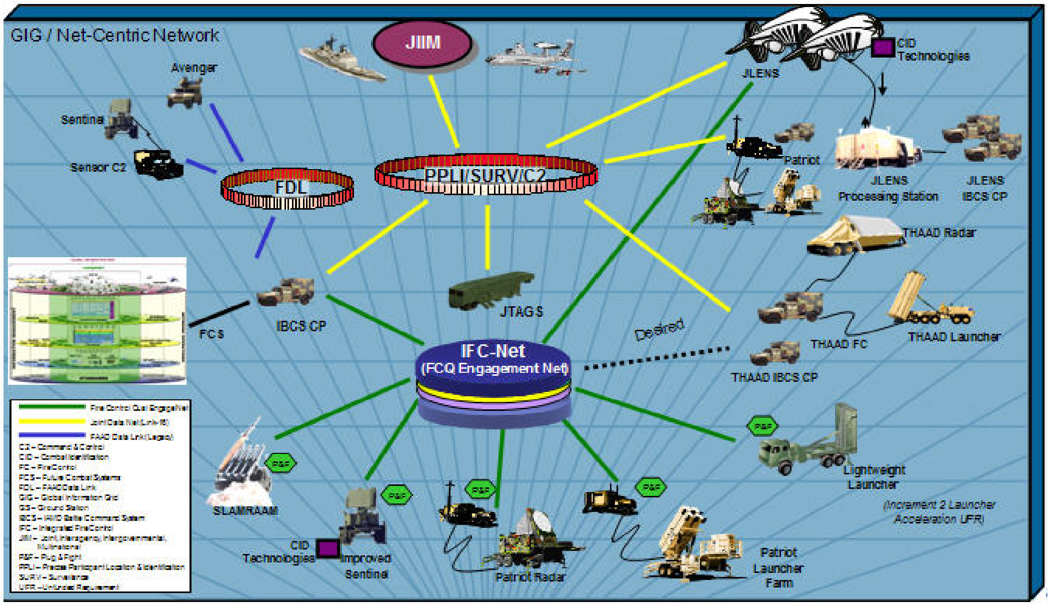


Figure 13. Army's Integrated Air Missile Defense System of Systems [From: IAMD Program Office, 2007]

C. INTEROPERABILITY

There is a continuum of interoperability from exchange of information in non-real time thru exchange of raw or semi-processed data as a stream that's being used and manipulated by multiple systems simultaneously. The nature of a mission or task gives rise to the type or degree of interoperability required between systems. With the move from system-centric to network-centric force operations, agreed to definitions for degrees of interoperability is key to the successful development and deployment of a specified network-centric capability.

A taxonomy of degrees of interoperability is useful in identifying critical functions and the technologies required to enable interoperability functions. These degrees of interoperability are pertinent to the definition of a relevant environment as well as definition of the type of system required.

A review of DoD, industry, and academic literature finds multiple approaches to defining the degree of interoperability. The literature review will encompass differing types of communication based on tasks or missions to be accomplished as a basis for defining degrees of interoperability.

DoD related literature is useful given the context of joint warfighting accomplished via connected systems. Academic literature contains advanced concepts and technologies not yet applied that may be useful in the future. The commercial industry literature provides the perspective of interoperability via standards that are generally required for a profitable business.

Interoperability is concerned with connectivity, capacity, consistency, bandwidth usage, data latency, syntactic compatibility, and undesirable semantic emergent behavior (DiMario, 2006). Interoperability is the context in which a SoS definition will be defined. An appropriate SoS definition will define the proper operational relevant environment in which a TRA is conducted to assess the ability and maturity of a technology to support the degree of interoperability required.

1. DoD/Government Literature Summary

The Joint Publication 1, ‘Doctrine for the Armed Forces of the United States’ states that unified action demands maximum interoperability - The forces, units, and systems of all Services must operate together effectively (Joint Chiefs of Staff, 2007) and that interoperability should be achieved primarily by a commonality of equipment, software, and systems both horizontally and vertically (Joint Chiefs of Staff, 2006). This effectiveness is enabled in part through the use of joint and/or interoperable communications and information systems that are developed based on a capability-focused, effects-based approach to advance Information Technology (IT) and National Security Systems (NSS) interoperability (Assistant Secretary of Defense for Networks and Information Integration/Department of Defense Chief Information Officer, 2004). DoD established a KPP for IT systems. The Interoperability KPP that was originally defined has been replaced by the Net-Ready (NR) KPP. The NR KPP is used to assess net-ready attributes required for both the technical exchange of information and the end-to-end operational effectiveness of that exchange. Meeting the NR KPP was established to assure coherent behavior of the interconnected systems to accomplish a common mission or task.

The DoD definitions of interoperability are:

> 1.The ability to operate in synergy in the execution of assigned tasks. 2. The condition achieved among communications-electronics systems or items of communications-electronics equipment when information or services can be exchanged directly and satisfactorily between them and/or their users. The degree of interoperability should be defined when referring to specific cases (Joint Chiefs of Staff, 2001 as amended through 2007).

A mental model for network-centric operations and interoperability has been proposed by Alberts et al. (see Figure 15). He proposes the following independent technical performance metrics to characterize interoperability (Alberts et al., 2001):

- Completeness (are all the relevant items available, including entities, their attributes, and relationships between them)
- Correctness (are all the items in the system faithful representations of the realities they describe)
- Currency (age of the items of information, often termed their latency)

- Accuracy or Level of Precision (which is conditional on the purpose the user has in mind)
- Consistency across different command centers, functionally specialized arenas, and applications

The model shows the system functions of collection/analysis (sense), decision making/C2 (control) and execution (engage) overlaid with the idea of sharing and collaboration to accomplish these functions within a networked force. Sharing is accomplished today via tactical data links. Collaboration to enable synchronization of systems for flexible engagements with an emphasis staying inside the enemies' engagement timeline is the promise of network-centric operations.

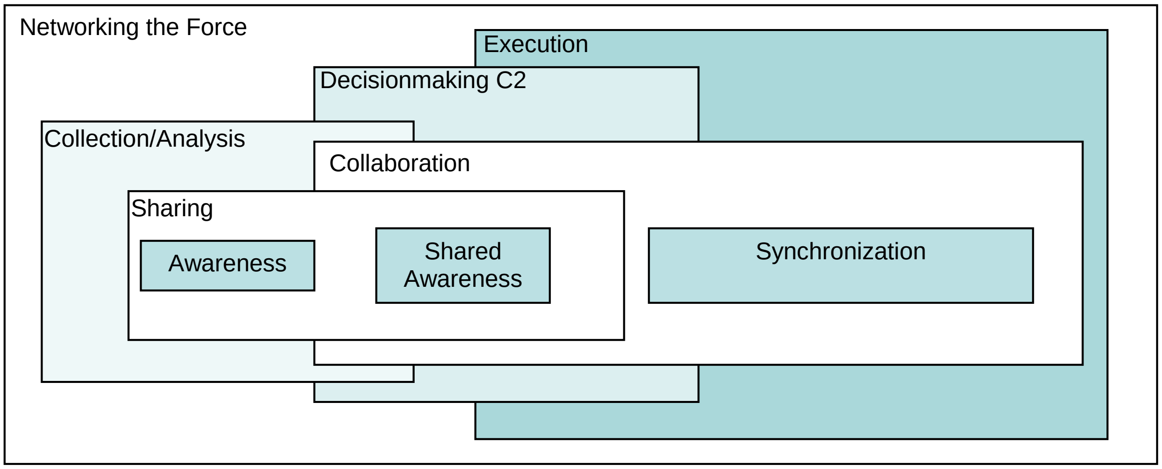


Figure 14. Networking the Force Mental Model [From: Alberts et al., 2001]

The collaborative functions that are required to enable synchronization are the following (Alberts et al., 2001):

- Inclusive: all the relevant actors are involved
- Collaboration across organizational, functional, spatial, and temporal boundaries, including echelons of command
- Multi-connected (every actor has access to all other actors)
- Unrestricted communication (between the collaborators)
- Participatory (all relevant actors are engaged in the process)
- Continuous (actors are engaged without disruption)
- Simultaneous (synchronous)

- Media-rich (face-to-face, with shared images, information, and data)
- Domain-rich (involves both the cognitive and the information domains)
- Content-rich (involves data, information, knowledge, and understandings)

Interoperability enables Force multiplication and is accomplished through common command, control, communications, computers, intelligence, surveillance and reconnaissance (C4ISR) specifications, integrated functionality, universal data models and other means to enable information sharing and data combining/fusion (Christiansen, 2005). The DoD mandate for network-centricity as developed and fielded in each system empowers users with the ability to easily discover, access, integrate, correlate and fuse data/information that support their mission objectives unconstrained by geospatial location or time of day (Zavin, 2005). Figure 16 shows the ideal interoperability to realize which enables the shortest successful engagement timelines for the lowest cost.

Not all missions require such tightly coupled operations or collaboration. The mission and specific task within a mission will drive the degree of interoperability. The mission/task can be accomplished through the allocation and aggregation of individuals, organizations, systems, infrastructure, and processes to create and share the data, information, and knowledge needed to plan, execute, and assess joint force operations and to enable a commander to make decisions better and faster than the adversary (United States Joint Forces Command, 2004).

The Department of Navy (DoN) may have the most challenging interoperability problem given the geospatial span of their systems across space, air, surface, land, and subsurface. The Navy typically develops and fields multi-mission systems which use common planning, C4ISR and weapon system components to conduct multiple missions simultaneously. Enabling collaboration across major missions with multiple platforms allows the DoN to conserve resources and maximize force multiplication. In addition Navy has the challenge of being interoperable with the other Services; the ASN(RDA) CHENG depicts the joint interoperability challenge of Navy with the other Services as seen in Figure 17.

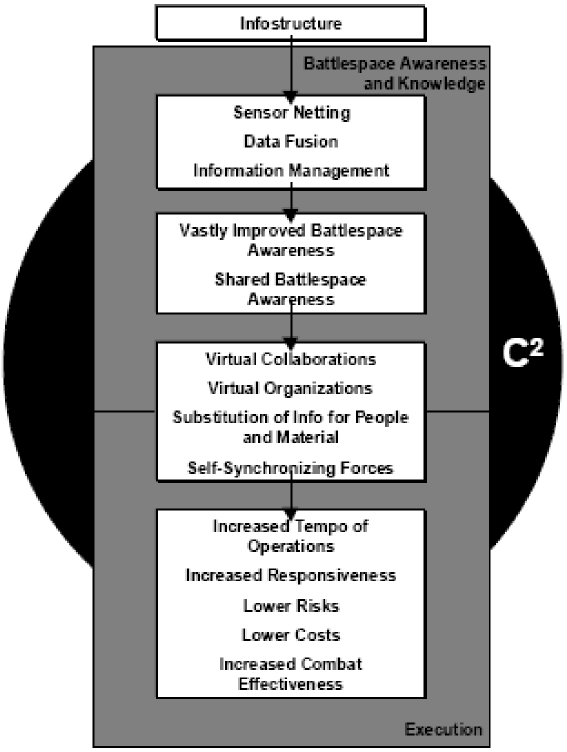
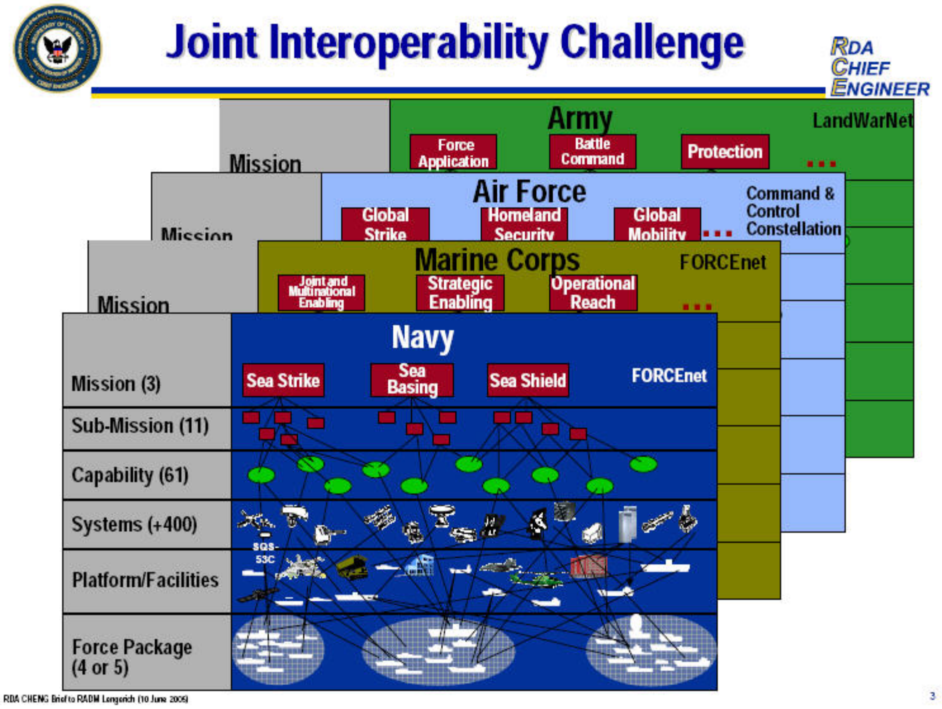

Infostructure
Battlespace Awareness and Knowledge
Sensor Netting
Data Fusion
Information Management
Vastly Improved Battlespace Awareness
Shared Battlespace Awareness
Virtual Collaborations
Virtual Organizations
Substitution of Info for People and Material
Self-Synchronizing Forces
Increased Tempo of Operations
Increased Responsiveness
Lower Risks
Lower Costs
Increased Combat Effectiveness
Execution
C²

Figure 15. The Military as a Network-Centric Enterprise [From: Alberts et al., 1999]

Given that the warfighter requires interoperability and mission and specific task within a mission drives the degree of interoperability, all systems may not need to be tightly coupled. An interoperability distinction among DoD systems being loosely coupled and tightly coupled would need to be made. A tightly coupled set of systems would be characterized by interfaces that provide for data and information sharing in the interest of cooperation and collaboration usually in near-real time and real-time. An example is the Army's Future Combat System that provides for a networked set of systems that in cooperation and collaboration are able to shorten timelines for sense, control and engagement of the enemy (Future Combat System Program Office, 2007). A loosely coupled set of systems would be characterized by interfaces that provide for data and information sharing in the interest of coordination in non-real time or near real-time. Examples are the various tactical data links that pass information about an entity's location and message traffic that provides mission planning information and other non-real time data and information regarding daily events and affairs.



Joint Interoperability Challenge

RDA CHIEF ENGINEER

Army
LandWarNet
Mission
Force Application
Battle Command
Protection
. . .

Air Force
Command & Control Constellation
Mission
Global Strike
Homeland Security
Global Mobility
. . .

Marine Corps
FORCEnet
Mission
Joint and Multinational Enabling
Strategic Enabling
Operational Reach
. . .

Navy
FORCEnet
Mission (3)
Sea Strike
Sea Basing
Sea Shield
Sub-Mission (11)
Capability (61)
Systems (+400)
SQS-53C
Platform/Facilities
Force Package (4 or 5)

RDA CHENG Brief to RADM Lengerich (10 June 2006)

3

Figure 16. Department of Navy Interoperability Challenge [From: Siel, 2006]

2. Non DoD Industry Literature Summary

In the commercial world, Information Technology (IT) businesses are best built using agreed to standards whether databases, telecommunications, or computer operating systems. An applicable example is the set of standards for the internet called Request for Comments (RFC) held in a repository maintained by the Internet Engineering Task Force (IETF) Secretariat. The IETF is a large open international community of network designers, operators, vendors, and researchers concerned with the evolution of the Internet architecture and the smooth operation of the Internet (IETF, 2007). RFCs are the community agreed to standardization of protocols and procedures on networking that began in 1969 as part of the original Advance Research Program Agency wide-area networking (ARPANET) project. The RFC standards are related to the Open Systems Interconnection Initiative (OSI) 7 layer model for networking established by the International Standards Organization (ISO). The OSI model provides for ‘services’ that are a layered, abstract description for communications and computer network protocol design. The layers are defined as follows (Subramanian, 2000):

Application (Layer 7): This layer supports application and end-user processes. Communication partners are identified, quality of service is identified, user authentication and privacy are considered, and any constraints on data syntax are identified. Everything at this layer is application-specific. This layer provides application services for file transfers, e-mail, and other network software services. Telnet and FTP are applications that exist entirely in the application level. Tiered application architectures are part of this layer.

Presentation (Layer 6): This layer provides independence from differences in data representation (e.g., encryption) by translating from application to network format, and vice versa. The presentation layer works to transform data into the form that the application layer can accept. This layer formats and encrypts data to be sent across a network, providing freedom from compatibility problems. It is sometimes called the syntax layer.

Session (Layer 5): This layer establishes, manages and terminates connections between applications. The session layer sets up, coordinates, and terminates conversations, exchanges, and dialogues between the applications at each end. It deals with session and connection coordination.

Transport (Layer 4): This layer provides transparent transfer of data between end systems, or hosts, and is responsible for end-to-end error recovery and flow control. It ensures complete data transfer.

Network (Layer 3): This layer provides switching and routing technologies, creating logical paths, known as virtual circuits, for transmitting data from node to node. Routing and forwarding are functions of this layer, as well as addressing, internetworking, error handling, congestion control and packet sequencing.

Data Link (Layer 2): At this layer, data packets are encoded and decoded into bits. It furnishes transmission protocol knowledge and management and handles errors in the physical layer, flow control and frame synchronization. The data link layer is divided into two sub-layers: The Media Access Control (MAC) layer and the Logical Link

Control (LLC) layer. The MAC sublayer controls how a computer on the network gains access to the data and permission to transmit it. The LLC layer controls frame synchronization, flow control and error checking.

Physical (Layer 1): This layer conveys the bit stream -- electrical impulse, light or radio signal -- through the network at the electrical and mechanical level. It provides the hardware means of sending and receiving data on a carrier, including defining cables, cards and physical aspects. Fast Ethernet, RS232, and ATM are protocols with physical layer components.

3. Academia Literature Summary

The Carnegie Mellon's Software Engineering Institute (SEI) is a federally funded research and development center conducting software engineering research in software system acquisition, architecture, products and interoperability (Carnegie Mellon Software Engineering Institute, 2007). SEI has an extensive partner network that stretches beyond DoD and for this thesis and literature review is treated as an academic organization that works extensively with other academic and commercial industry partners in addition to DoD.

SEI defines interoperability as:

> The ability of a collection of communicating entities to (a) share specified information and (b) operate on that information according to a shared operational semantics in order to achieve a specified purpose in a given context." SEI cites DoD references for definitions of operational interoperability "the ability of systems, units, or forces to provide services to and accept services from other systems, units, or forces and to use the services so exchanged to enable them to operate effectively together (Kasunic and Anderson, 2004).

The Software Engineering Institute developed a model called Levels of Information Systems Interoperability (LISI) (See Figure 18). It was used for a while as a representative model for DoD Interoperability KPP. The SEI's LISI model proposes a taxonomy of interoperability: Isolated – non-connected with manual inputs, Connected – electronic connection with separate data and applications using homogeneous data exchange mechanisms, Functional – minimal common functions with separate data and applications using heterogeneous data exchange for basic collaboration, Domain – shared data with separate applications using shared databases, and Enterprise – interactive manipulation with shared data and applications using automated distributed information exchange applications. The LISI model discriminates among incremental levels of information exchange and shared applications (C4ISR Architecture Working Group, 1997).

The specific capabilities needed to achieve each level were described in terms of four attributes – procedures, applications, infrastructure, and data as follows (C4ISR Architecture Working Group, 1997):

- Procedures: guidance that impact system interoperability, including doctrine, mission, architectures, and standards.
- Applications: functions manifest in the system's software components, from single processes to integrated applications suites.
- Infrastructure: components that enable interactions between systems, including hardware, communications, system services, and security. For example, infrastructure considers the protocols, enabling software services, and supporting data structures for information flow between applications and data.
- Data: includes the data formats and standards that support interoperability at all levels. It embodies the entire range of styles and formats from simple text to enterprise data models.

The literature review regarding interoperability did not reveal an agreed to definition or a standard taxonomy of degrees of interoperability. Therefore, a back to basics approach was taken to define the types of communication or the purposes of communication as a strategy to get to what are the degrees of interoperability.

Control (LLC) layer. The MAC sublayer controls how a computer on the network gains access to the data and permission to transmit it. The LLC layer controls frame synchronization, flow control and error checking.

Physical (Layer 1): This layer conveys the bit stream - electrical impulse, light or radio signal -- through the network at the electrical and mechanical level. It provides the hardware means of sending and receiving data on a carrier, including defining cables, cards and physical aspects. Fast Ethernet, RS232, and ATM are protocols with physical layer components.

3. Academia Literature Summary

The Carnegie Mellon's Software Engineering Institute (SEI) is a federally funded research and development center conducting software engineering research in software system acquisition, architecture, products and interoperability (Carnegie Mellon Software Engineering Institute, 2007). SEI has an extensive partner network that stretches beyond DoD and for this thesis and literature review is treated as an academic organization that works extensively with other academic and commercial industry partners in addition to DoD.

SEI defines interoperability as:

> The ability of a collection of communicating entities to (a) share specified information and (b) operate on that information according to a shared operational semantics in order to achieve a specified purpose in a given context." SEI cites DoD references for definitions of operational interoperability "the ability of systems, units, or forces to provide services to and accept services from other systems, units, or forces and to use the services so exchanged to enable them to operate effectively together (Kasunic and Anderson, 2004).

The Software Engineering Institute developed a model called Levels of Information Systems Interoperability (LISI) (See Figure 18). It was used for a while as a representative model for DoD Interoperability KPP. The SEI's LISI model proposes a taxonomy of interoperability: Isolated – non-connected with manual inputs, Connected – electronic connection with separate data and applications using homogeneous data exchange mechanisms, Functional – minimal common functions with separate data and applications using heterogeneous data exchange for basic collaboration, Domain – shared

Coordinate – to bring into a common action, movement, or condition (Merriam-Webster, 2007), Cooperate - to act or work with another or others**:** act together or in compliance (Merriam-Webster, 2007), Collaborate - to work jointly with others or together (Merriam-Webster, 2007), Direct - to regulate the activities or course of (Merriam-Webster, 2007).

These differing purposes lead to differing types of data, information, and knowledge flow as well as differing timings.

D. TECHNOLOGY READINESS ASSESSMENTS

What is technology and why and how is it assessed. From Merriam's-Webster online (Merriam-Webster, 2007) dictionary, technology comes from the Greek technologia, which is a systematic treatment of an art, from technē art, skill + -o- + -logia –logy, date: 1859. Its definition includes:

> …the practical application of knowledge especially in a particular area; a capability given by the practical application of knowledge; a manner of accomplishing a task especially using technical processes, methods, or knowledge.

Most useful may be the idea of technology as a realization of a specific tool, technique or method that may be applied consistently to solve a specified problem or create something new.

NASA's Technology plan defines technology as follows (Bilbro, 2006):

> Technology is defined as the practical application of knowledge to create the capability to do something entirely new or in an entirely new way. This can be contrasted to scientific research, which encompasses the discovery of new knowledge from which new technology is derived, and engineering which uses technology derived from this knowledge to solve specific technical problems.

Technology can rarely be developed to a specified schedule and breakthrough technologies are rarely available to support a program schedule. Failure to account for the time to develop technology contributes significantly to schedule slip and cost overrun for a program. Even if a technology has been fielded in one system doesn't mean that it is mature enough to meet the requirements of another system or meet SoS requirements.

Most IT technologies that have been fielded in a system must be modified to work in an enterprise or SoS/IT application. Technology assessments are used to identify the development activities and risks associated with technology development in support of a program.

The formalization of technology assessments within the government was started by NASA. John C. Mankins, of NASA, first documented Technology Readiness Levels (TRLs) in his white paper 'Technology Readiness Levels, A White Paper,' April 6, 1995 (Mankins, 1995).

This literature review will include the DoD's TRA Deskbook, GAO reports, NASA technology assessment approaches and Service specific technology assessment strategies and initiatives. In addition, personal participation and observation in the execution of the DoD's first Joint SoS TRA will be included. Most of the documented information regarding technology assessment is within DoD and NASA; however, this review will include personal observations of the non-DoD Industry. In particular, guidance that would be pertinent to a SoS TRA is included.

1. Technology Readiness Assessment Government/Department of Defense Industry Literature Review

The definition of a TRA per the TRA Deskbook:

> …is a systematic, metrics-based process and accompanying report that assesses the maturity of certain technologies [(called Critical Technology Elements (CTEs)) used in systems." The TRA report includes "how the CTEs are identified, why they are important to the program and an independent assessment of their maturity ((DUSD(S&T)), 2005).

There has been an increased interest by Congress and Office of Secretary of Defense on managing programs within cost, schedule and performance. One of the contributors to delays and cost overruns is the use of immature technologies. DoD Directive Number 5000.1 May12, 2003, The Defense Acquisition System, USD(AT&L), DoD Instruction Number 5000.2 May 12, 2003, Operation of the Defense Acquisition System, USD(AT&L) and DoD Acquisition Guidebook, Last Modified on: 12/20/2004 (USD(AT&L), 2006), section 10.5.2 gives guidance regarding Technology Readiness Assessments (TRAs) to support program initiation for ships (usually Milestone A, Milestone B (typical program initiation) and Milestone C (system/product production) decisions. Formal, independent TRAs approved by a Service S&T Executive and the Service Acquisition Executive are required for MDAP and MAIS acquisitions. The latest TRA Deskbook dated May 2005, prepared by the Deputy Under Secretary of Defense for Science and Technology (DUSD(S&T)) provides the latest instructions and guidance for TRAs. TRAs should be conducted for each block or spiral of an acquisition program. All of these documents are basically silent on FoS TRAs and include very little guidance on SoS TRAs.

In the early 1990s, DoD adopted NASA's Technology Readiness Level (TRLs) scale (see Figure 19) with minor modifications and developed a TRA Deskbook containing guidance and best practices on technology development and assessment using these TRLs. Detailed descriptions of the Hardware TRLs can be found in Table 1. NASA's TRLs developed during the 1970's and 1980's were primarily applied to hardware programs. In the last twenty years, software development has become more prevalent. The hardware TRLs have been modified to reflect the aspect of software maturity. Both NASA and DoD have developed software TRLs. See Figure 20 for NASA's software TRLs and Table 2. for DoD descriptions of software TRLs. Terms used in these descriptions such as breadboard and high fidelity environment are defined just after Table 2.

Software is mostly associated with IT systems. The TRA Deskbook and Gold and Jabubek in their article 'Technology Readiness Assessments for IT and IT-Enabled Systems' ((DUSD(S&T)), 2005) and (Gold and Jakubak, 2005), define four types of IT systems:

- Business systems – off-the-shelf information system components and COTS software assembled together in a new environment to support the business and management functions of an organization
- Net-reliant (battle management) systems – typically command and control; battle management systems; or intelligence, surveillance, and reconnaissance systems. The net-reliant system is characterized by an intense real-time requirement

- Network infrastructure (or services provider) - backbone and services systems for network management, management of large databases and glue logic to execute and retrieve services across a Wide Area Network of varying security levels.
- Embedded systems - functionality is enabled by IT but not driven by IT itself. Embedded systems emphasize using computer hardware and software to automate internal functions of a weapon system such as platform control and status, sensor signal and data processing, and weapons tasking.

Over time DoD has developed TRLs for other categories such as manufacturing and medical. Details of the DoD manufacturing and medical TRLs can be found in the TRA Deskbook.

Assessment begins by identifying the operational environment and the KPPs and other required capabilities for a system. As the system is engineered those technologies that enable the meeting of operational requirements in the environment that the system will be employed, support manufacturing of hardware or development of software (e.g., Integrated Development Environment) are identified. Key drivers of the operational environment must be identified, so that demonstration and test results of a CTE are analyzed with respect to these drivers. CTEs are assessed using the appropriate TRLs. CTEs include hardware, software, algorithms, techniques, and methods. Assessments are conducted throughout system acquisition. The following applies per the TRA Deskbook.

For a technology to be critical, the answer to one of the following questions must be ‘yes’:

- Does the technology directly impact an operational requirement?
- Does the technology have a significant impact on an improved delivery schedule?
- Does the technology have a significant effect on the system’s affordability?
- If this is a spiral development, is the technology essential to meet the spiral deliverables?

In addition, the answer to one of the following questions must also be ‘yes’:

- Is the technology new or novel?
- Is the technology modified?

- Has the technology been repackaged so that a new relevant environment is realized?
- Is the technology expected to operate in an environment and/or achieve a performance beyond its original design intention or demonstrated capability?

Identification of the operational relevant environments will like include the following ((DUSD(S&T)), 2005):

- Physical Environment. Including but not limited to: mechanical components, processors, servers, and electronics; kinetic and kinematic; thermal and heat transfer; electrical and electromagnetic; climatic—weather, temperature, particulate; network infrastructure
- Logical Environment. Including but not limited to: software (algorithm) interfaces; security interfaces; Web-enablement
- Data Environment. Including but not limited to: data formats and databases; anticipated data rates, data delay and data throughput; data packaging and framing
- Security Environment. Including but not limited to: connection to firewalls; security appliqués; rates and methods of attack
- User and Use Environment. Including but not limited to: scalability; upgradability; user behavior adjustments; user interfaces; organizational change/realignments with system impacts; implementation plan.

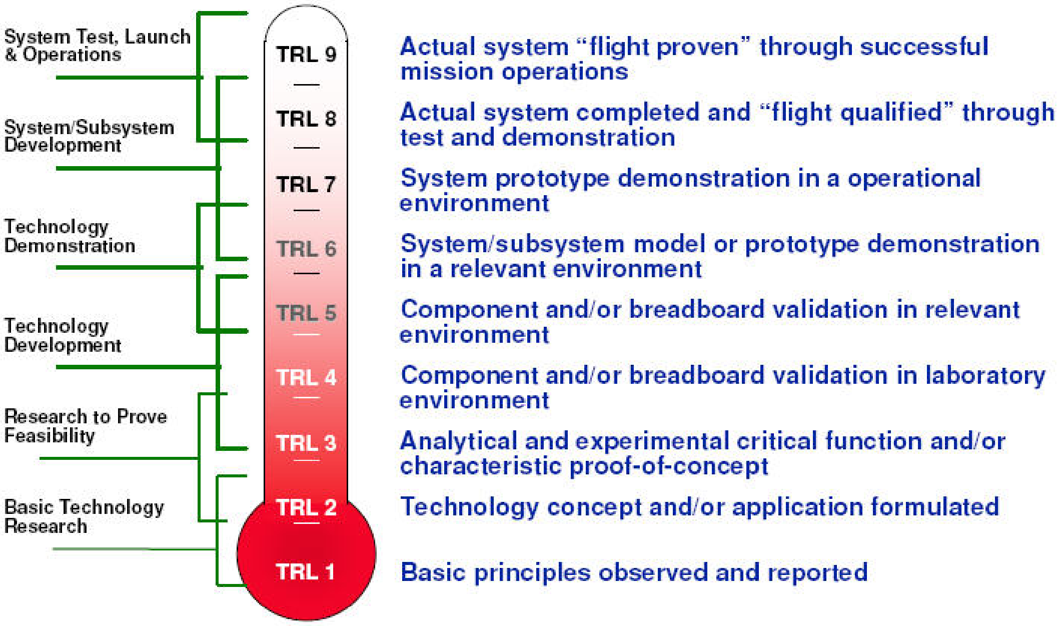
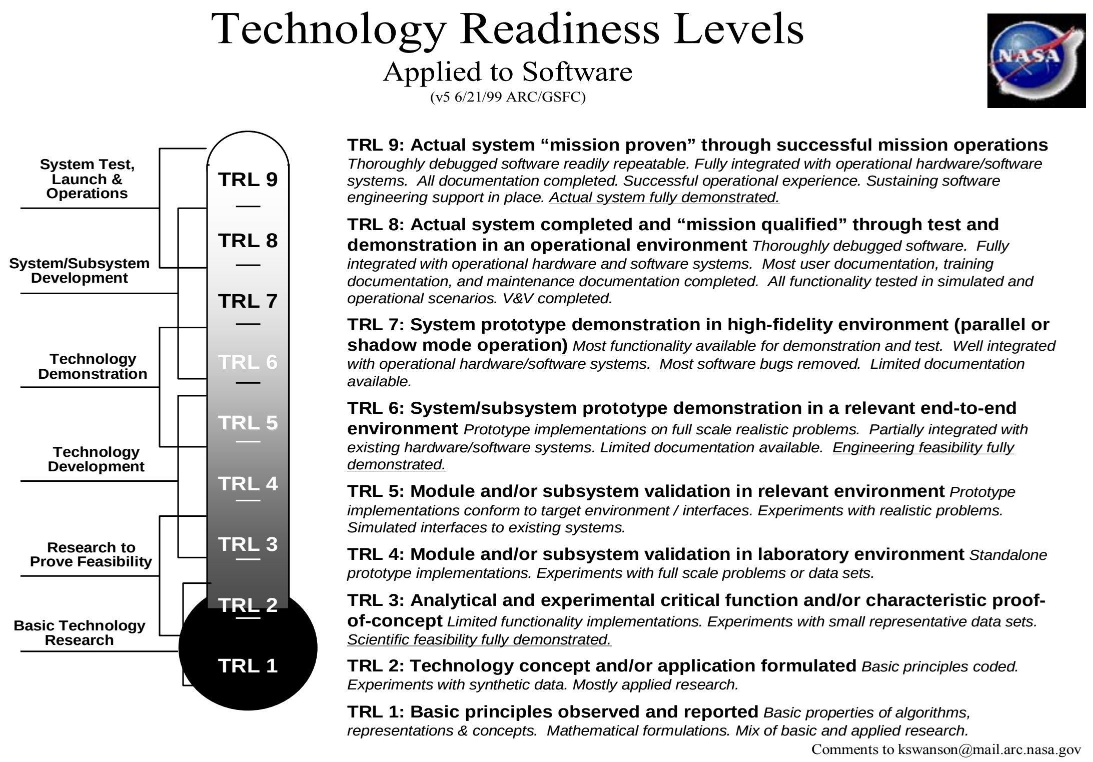

System Test, Launch & Operations
System/Subsystem Development
Technology Demonstration
Technology Development
Research to Prove Feasibility
Basic Technology Research
TRL 9
TRL 8
TRL 7
TRL 6
TRL 5
TRL 4
TRL 3
TRL 2
TRL 1
Actual system "flight proven" through successful mission operations
Actual system completed and "flight qualified" through test and demonstration
System prototype demonstration in a operational environment
System/subsystem model or prototype demonstration in a relevant environment
Component and/or breadboard validation in relevant environment
Component and/or breadboard validation in laboratory environment
Analytical and experimental critical function and/or characteristic proof-of-concept
Technology concept and/or application formulated
Basic principles observed and reported

Figure 18. Hardware Technology Readiness Level (TRL) scale [From: National Aeronautics and Space Administration, 2007]

H/W TRL	DEFINITION	DESCRIPTION	SUPPORT INFORMATION
1	Basic principles observed and reported.	Lowest level of technology readiness. Scientific research begins to be translated into applied research and development (R&D). Examples might include paper studies of a technology's basic properties.	Published research that identifies the principles that underlie this technology. References to who, where, when.
2	Technology concept and/or application formulated.	Invention begins. Once basic principles are observed, practical applications can be invented. Applications are speculative, and there may be no proof or detailed analysis to support the assumptions. Examples are limited to analytic studies. Once basic principles are observed, practical applications can be invented. Applications are speculative, and there may be no proof or detailed analysis to support the assumptions. Examples are limited to analytic studies using synthetic data	Publications or other references that outline the application being considered and that provide analysis to support the concept. Applied research activities, analytic studies, small code units, and papers comparing competing technologies.
3	Analytical and experimental critical function and/or characteristic proof of concept.	Active R&D is initiated. This includes analytical studies and laboratory studies to physically validate the analytical predictions of separate elements of the technology. Examples include components that are not yet integrated or representative.	Results of laboratory tests performed to measure parameters of interest and comparison to analytical predictions for critical subsystems. References to who, where, and when these tests and comparisons were performed.
4	Module and/or subsystem validation in a laboratory environment (i.e., software prototype development environment).	Basic technological components are integrated to establish that they will work together. This is relatively "low fidelity" compared with the eventual system. Examples include integration of "ad hoc" hardware in the laboratory.	System concepts that have been considered and results from testing laboratory scale breadboard(s). References to who did this work and when. Provide an estimate of how breadboard hardware and test results differ from the expected system goals.
5	Module and/or subsystem validation in a relevant environment.	Fidelity of breadboard technology increases significantly. The basic technological components are integrated with reasonably realistic supporting elements so they can be tested in a simulated environment. Examples include "high fidelity" laboratory integration of components.	Results from testing a laboratory breadboard system are integrated with other supporting elements in a simulated operational environment. How does the "relevant environment" differ from the expected operational environment? How do the test results compare with expectations? What problems, if any, were encountered? Was the breadboard system refined to more nearly match the expected system goals?

H/W TRL	DEFINITION	DESCRIPTION	SUPPORT INFORMATION
6	Module and/or subsystem validation in a relevant end-to-end environment.	Representative model or prototype system, which is well beyond that of TRL 5, is tested in a relevant environment. Represents a major step up in a technology's demonstrated readiness. Examples include testing a prototype in a high fidelity laboratory environment or in a simulated operational environment.	Results from laboratory testing of a prototype system that is near the desired configuration in terms of performance, weight, and volume. How did the test environment differ from the operational environment? Who performed the tests? How did the test compare with expectations? What problems, if any, were encountered? What are/were the plans, options, or actions to resolve problems before moving to the next level?
7	System prototype demonstration in an operational high-fidelity environment.	Prototype near or at planned operational system. Represents a major step up from TRL 6 by requiring demonstration of an actual system prototype in an operational environment (e.g., in an aircraft, in a vehicle, or in space). Examples include testing the prototype in a test bed aircraft.	Results from testing a prototype system in an operational environment. Who performed the tests? How did the test compare with expectations? What problems, if any, were encountered? What are/were the plans, options, or actions to resolve problems before moving to the next level?
8	Actual system completed and mission qualified through test and demonstration in an operational environment.	Technology has been proven to work in its final form and under expected conditions. In almost all cases, this TRL represents the end of true system development. Examples include developmental test and evaluation of the system in its intended weapon system to determine if it meets design specifications.	Results of testing the system in its final configuration under the expected range of environmental conditions in which it will be expected to operate. Assessment of whether it will meet its operational requirements. What problems, if any, were encountered? What are/ were the plans, options, or actions to resolve problems before finalizing the design?
9	Actual system proven through successful mission-proven operational capabilities.	Actual application of the technology in its final form and under mission conditions, such as those encountered in operational test and evaluation (OT&E). Examples include using the system under operational mission conditions.	OT&E reports.

Table 1. Hardware Technology Readiness Level Descriptions [From: (DUSD(S&T)), 2005]



Technology Readiness Levels

Applied to Software

(v5 6/21/99 ARC/GSFC)

System Test, Launch & Operations
System/Subsystem Development
Technology Demonstration
Technology Development
Research to Prove Feasibility
Basic Technology Research
TRL 9
TRL 8
TRL 7
TRL 6
TRL 5
TRL 4
TRL 3
TRL 2
TRL 1
NASA

TRL 9: Actual system "mission proven" through successful mission operations *Thoroughly debugged software readily repeatable. Fully integrated with operational hardware/software systems. All documentation completed. Successful operational experience. Sustaining software engineering support in place. Actual system fully demonstrated.*

TRL 8: Actual system completed and "mission qualified" through test and demonstration in an operational environment *Thoroughly debugged software. Fully integrated with operational hardware and software systems. Most user documentation, training documentation, and maintenance documentation completed. All functionality tested in simulated and operational scenarios. V&V completed.*

TRL 7: System prototype demonstration in high-fidelity environment (parallel or shadow mode operation) *Most functionality available for demonstration and test. Well integrated with operational hardware/software systems. Most software bugs removed. Limited documentation available.*

TRL 6: System/subsystem prototype demonstration in a relevant end-to-end environment *Prototype implementations on full scale realistic problems. Partially integrated with existing hardware/software systems. Limited documentation available. Engineering feasibility fully demonstrated.*

TRL 5: Module and/or subsystem validation in relevant environment *Prototype implementations conform to target environment / interfaces. Experiments with realistic problems. Simulated interfaces to existing systems.*

TRL 4: Module and/or subsystem validation in laboratory environment *Standalone prototype implementations. Experiments with full scale problems or data sets.*

TRL 3: Analytical and experimental critical function and/or characteristic proof-of-concept *Limited functionality implementations. Experiments with small representative data sets. Scientific feasibility fully demonstrated.*

TRL 2: Technology concept and/or application formulated *Basic principles coded. Experiments with synthetic data. Mostly applied research.*

TRL 1: Basic principles observed and reported *Basic properties of algorithms, representations & concepts. Mathematical formulations. Mix of basic and applied research.*

Comments to kswanson@mail.arc.nasa.gov

Figure 19. NASA Software Technology Readiness Levels [From: NASA, 2007]

S/W TRL	DEFINITION	DESCRIPTION	SUPPORT INFORMATION
1	Basic principles observed and reported.	Lowest level of software technology readiness. A new software domain is being investigated by the basic research community. This level extends to the development of basic use, basic properties of software architecture, mathematical formulations, and general algorithms.	Basic research activities, research articles, peer-reviewed white papers, point papers, early lab model of basic concept may be useful for substantiating the TRL level.
2	Technology concept and/or application formulated.	Once basic principles are observed, practical applications can be invented. Applications are speculative, and there may be no proof or detailed analysis to support the assumptions. Examples are limited to analytic studies using synthetic data	Applied research activities, analytic studies, small code units, and papers comparing competing technologies.
3	Analytical and experimental critical function and/or characteristic proof of concept.	Active R&D is initiated. The level at which scientific feasibility is demonstrated through analytical and laboratory studies. This level extends to the development of limited functionality environments to validate critical properties and analytical predictions using nonintegrated software components and partially representative data.	Algorithms run on a surrogate processor in a laboratory environment, instrumented components operating in laboratory environment, laboratory results showing validation of critical properties.

S/W TRL	DEFINITION	DESCRIPTION	SUPPORT INFORMATION
4	Module and/or subsystem validation in a laboratory environment (i.e., software prototype development environment).	Basic software components are integrated to establish that they will work together. They are relatively primitive with regard to efficiency and robustness compared with the eventual system. Architecture development initiated to include interoperability, reliability, maintainability, extensibility, scalability, and security issues. Emulation with current/legacy elements as appropriate. Prototypes developed to demonstrate different aspects of eventual system.	Advanced technology development, stand-alone prototype solving a synthetic full-scale problem, or standalone prototype processing fully representative data sets.
5	Module and/or subsystem validation in a relevant environment.	Level at which software technology is ready to start integration with existing systems. The prototype implementations conform to target environment/interfaces. Experiments with realistic problems. Simulated interfaces to existing systems. System software architecture established. Algorithms run on a processor(s) with characteristics expected in the operational environment.	System architecture diagram around technology element with critical performance requirements defined. Processor selection analysis, Simulation/Stimulation (Sim/Stim) Laboratory buildup plan. Software placed under configuration management. COTS/GOTS in the system software architecture are identified.
6	Module and/or subsystem validation in a relevant end-to-end environment.	Level at which the engineering feasibility of a software technology is demonstrated. This level extends to laboratory prototype implementations on full-scale realistic problems in which the software technology is partially integrated with existing hardware/ software systems.	Results from laboratory testing of a prototype package that is near the desired configuration in terms of performance, including physical, logical, data, and security interfaces. Comparisons between tested environment and operational environment analytically understood. Analysis and test measurements quantifying contribution to system-wide requirements such as throughput, scalability, and reliability. Analysis of human-computer (user environment) begun.
7	System prototype demonstration in an operational high-fidelity environment.	Level at which the program feasibility of a software technology is demonstrated. This level extends to operational environment prototype implementations where critical technical risk functionality is available for demonstration and a test in which the software technology is well integrated with operational hardware/software systems.	Critical technological properties are measured against requirements in a simulated operational environment.
8	Actual system completed and mission qualified through test and	Level at which a software technology is fully integrated with operational hardware and software systems. Software development documentation is complete. All functionality tested in simulated and operational scenarios.	Published documentation and product technology refresh build schedule. Software resource reserve measured and tracked.

S/W TRL	DEFINITION	DESCRIPTION	SUPPORT INFORMATION
	demonstration in an operational environment.		
9	Actual system proven through successful mission- proven operational capabilities.	Level at which a software technology is readily repeatable and reusable. The software based on the technology is fully integrated with operational hardware/software systems. All software documentation verified. Successful operational experience. Sustaining software engineering support in place. Actual system.	Production configuration management reports. Technology integrated into a reuse “wizard”; out-year funding established for support activity.

Table 2. DoD Software Technology Readiness Levels [From: (DUSD(S&T)), 2005]

Definitions applicable to TRL descriptions ((DUSD(S&T)), 2005):

Breadboard: Integrated components that provide a representation of a system/subsystem and which can be used to determine concept feasibility and to develop technical data. Typically configured for laboratory use to demonstrate the technical principles of immediate interest. May resemble final system/subsystem in function only.

High Fidelity: Addresses form, fit and function. High-fidelity laboratory environment would involve testing with equipment that can simulate and validate all system specifications within a laboratory setting.

Low Fidelity: A representative of the component or system that has limited ability to provide anything but first order information about the end product. Low-fidelity assessments are used to provide trend analysis.

Model: A functional form of a system, generally reduced in scale, near or at operational specification. Models will be sufficiently hardened to allow demonstration of the technical and operational capabilities required of the final system.

Operational Environment: Environment that addresses all of the operational requirements and specifications required of the final system to include platform/packaging.

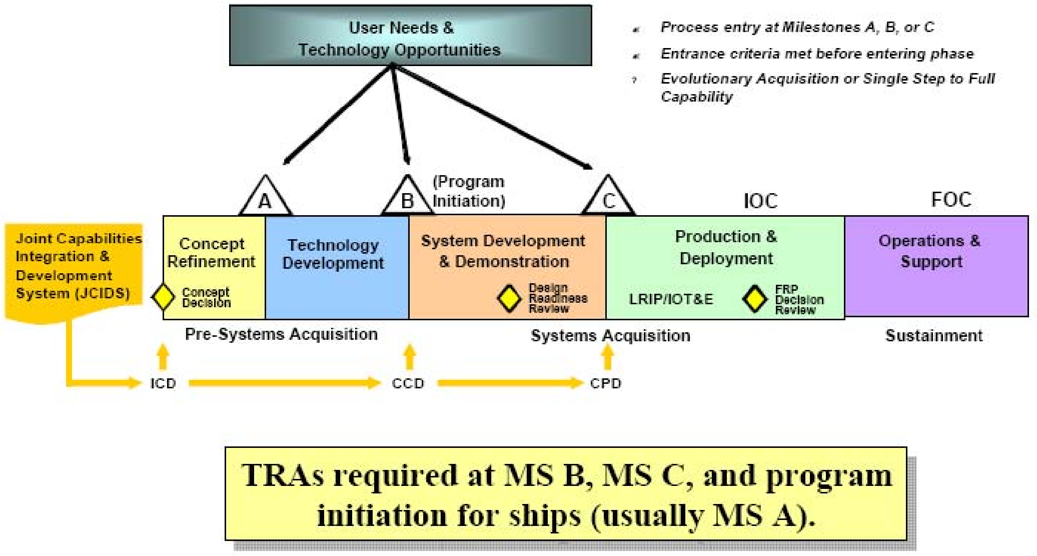
Prototype: A physical or virtual model used to evaluate the technical or manufacturing feasibility or military utility of a particular technology or process, concept, end item or system.

Relevant Environment: Testing environment that simulates the key aspects of the operational environment.

Simulated Operational Environment: Either 1) a real environment that can simulate all of the operational requirements and specifications required of the final system, or 2) a simulated environment that allows for testing of a virtual prototype; used in either case to determine whether a developmental system meets the operational requirements and specifications of the final system.

The TRA Deskbook recommends certain technology readiness by specific acquisition milestones to mitigate program risk (see Figure 21). It is required that the TRA be conducted by an independent panel of subject matter experts typically assembled by the component S&T Executive prior to a MS event. It is required that the TRA be conducted by and independent technology panel typically assembled by the component S&T Executive prior to a MS event. Assessments are made based on expert judgments and the technology design documentation, test results, and program requirements supplied by the PM.

Ideally, during the development of the Initial Capabilities Document (ICD) there should be involvement of the S&T community to ensure that materiel elements for the needed capabilities are plausible. At the beginning of concept development, alternatives are proposed and analyzed. During concept exploration there must be a balancing between required capabilities, cost, and availabilities of technologies. CTE technology development and/or modification is defined during the concept phase of a system and is restrained and constrained by system concepts of employment, Key Performance Parameters, System requirements (legacy constraints), and availability of money, time, and maturing Science and Technology (S&T) technologies and existing technologies. CTE should be assessed with respect to technology maturity and technical risk. Ideally, alternatives are based on technologies that typically are at least TRL 4 such that an evaluation of the expected performance and cost of a system alternative can be analyzed with moderate risk. If the system alternatives can not meet performance with technologies of at least TRL 4, ideally an S&T project is started for a technology area and the original program progresses with a lower performance requirement for its initial spirals or blocks.



TRAs required at MS B, MS C, and program initiation for ships (usually MS A).

Figure 20. Recommended Technology Readiness Assessments by Milestone [From: Mandelbaum, 2005]

At the same time, one should identify technology maturation plans and demonstration and test requirements required to be accomplished in the Technology Demonstration phase of the program and beyond. This information is required to develop the Technology Development Strategy (TDS), which is required at MS A. For new radars, ships, and other systems that have a long development times or long procurement/manufacture/build times and/or manufacturing facilities are required to be developed, it is paramount that critical technologies are identified very early during the concept stage. These technologies typically take an extraordinary long time to develop and require a significant investment.

In DoD it is common practice to develop or use advanced technologies to keep a warfighting edge. Advanced technologies will most likely be used in ways that have never been accomplished before. Historically, DoD PMs and their staffs have been too optimistic with regard to technology readiness and program schedules. Many programs actually progress without an S&T program and develop the technology within their program adding undo risk to their program. This is typically rationalized by the PM in order to meet program deadlines; the PM should coordinate and collaborate with the S&T community.

When a program is exiting the Technology Development phase and entering the SDD phase, the PM should be sure that the program is affordable and can be developed for production in a reasonable amount of time (typically less than five years); the statistics are against the PM being able to do this with immature technologies.

As a program nears Milestone B (~1 year prior), the Program Manager should formally propose the list of all CTEs to his respective Service's S&T Executive for approval. These should be easily identifiable from the system engineering artifacts related to functional architecture and the physical architecture which shows the system design broken down into all its subsystems and components. The program's work breakdown structure should be used (per acquisition guidance) to facilitate the enumeration of the CTEs. It is recommended that the list be inclusive of all technologies under consideration. For those technologies that have low TRLs, alternative technologies with higher TRLs should be included. The Program Manager (PM) should provide a draft technology readiness assessment to the Service S&T Executive and is required to defend the technology maturity levels claimed. It is the job of the S&T Executive to certify the TRA. This is accomplished for both MS B and MS C. Technologies are required to be a minimum of TRL6 for MS B and TRL 7 for MS C. There may be changes in the complement of technologies during program development. For technology assessments with respect to TRL 7, the environment should be the system in development. If no data/information exists under an operationally relevant environment, these activities must be conducted prior to MS C in order to have the data. It is the responsibility of the PM to keep the S&T Executive and TRA current on a regular basis.

Typical Questions that must be answered during a TRA:

1. Is this a new technology? Is the technology novel (a mature technology being used in a new way? Is the technology being modified or being used in a different environment? (Summarize what functions are being modified and how)?
2. Who developed the technology? When? Is it in another program? Is it fielded (for how long)?

3. What KPP(s) or operational requirements does this technology support? (i.e. Completeness, Clarity, Commonality, Net-Ready)
4. What documents exist that describe the technology and its performance? (State documents title and date and provide to panel)
5. What system and subsystem requirements are satisfied with this technology? What other technologies are used in conjunction with this technology to meet these requirements?
6. What functional capabilities does this technology map to?
7. What trade studies or concept papers exist for this technology element? (List name of trade study (date) and provide copy to panel)?
8. Brief Summary of Development products, architecture and system engineering artifacts as required.
9. Where was testing conducted? What scenarios/threats/ environments were used? Are the scenarios certified as representative of the operational environment? How were these tailored to test technology components not in a development system? What artifacts are available (provide those available)? What was the performance with respect to the requirements?
10. When will development and testing be complete at a subsystem, system, and SoS levels.

The TRL descriptions and supporting information should be tailored with program specific details. This allows program personnel to communicate clearly about what specific steps are required to mature a technology. See Table 3 for an example. The TRA Deskbook provides many good examples of this annotation as well as details relevant to assessments of specific types of hardware, software/IT, manufacturing and biomedical technologies.

TRL	Example Description
5	**Strategies identified to mitigate technical and cost risk:** Change from 2-in. to 4-in. wafers for Molecular Beam Epitaxy (MBE) growth. Identify machines to automate bar stacking in coating fixtures. Preload bars in bonding fixtures to reduce solder thickness in laser diode array package and improve reliability and thermal performance

Table 3. Example of TRL tailoring [From: (DUSD(S&T)), 2005]

The following content from the TRA Deskbook is applicable for SoS TRAs:

- Software CTE identification and assessment typically includes algorithms/ techniques/methods, components, subsystem, system/program/package, and SoS elements. The environment description should include integration aspects, user environment, logical relationships, data environment, and external interfaces.

- CTEs are most likely found performing functions supporting synchronization, timeliness, accuracy, dissemination and consistency of data requirements, operating system environment, workstations, servers, other special processing needs and Quality of Service and throughput of networks.
- IT systems engineering creates a data model that exposes data types and their relationships. This data model includes a description of data flow (i.e., how the activities of the IT system affect the data) and the distribution of computational processes over the system. The data model is analogous to the functional architecture for a hardware-centric system.
- Consider the following during the assessment: obsolescence, scalability, data storage, number and type of applications, processor requirements and throughput including appropriate hardware components that are required to meet these requirements.
- Specifically identify and assess Commercial-off-the-Shelf (COTS) and industry standards and their ability to support military needs (including but not limited to reliability, availability, and security) over the long term without undo modification and costs.
- Claiming technical readiness in an operation environment (TRL 7 or higher) requires a detailed architecture that fully exposes all components and elements affecting the operation of the critical software element. Claiming technical readiness in a relevant environment (TRL 6 or higher) requires evidence of the acceptable performance of the software element under operational factors, including, for example, system loading, user interaction, and realistic communications environment (e.g., bandwidth, latency, jitter). In other words, claiming a TRL 5 or higher requires a detailed architecture, and claiming a TRL 7 or higher requires, in addition to the detailed architecture, defining the operational environment and evidence of acceptable performance in the operational environment.

There are a variety of methods used across DoD by the Services to better assess technology readiness. Two exemplars are included in this thesis. The Missile Defense Agency (MDA) has developed a detailed checklist for each TRL both hardware and software. The MDA hardware TRL checklist in included as Table 3. MDA has clarified specific steps that must be met to clearly move to the next level of readiness. MDA also has a draft Software TRL checklist similar to the Hardware TRL checklist included here.

TECHNOLOGY READINESS LEVEL 1 HARDWARE MATURITY CHECKLIST		
DoD TRL 1 Definition	**TRL 1 Hardware Maturity Criteria**	**Certification Authority**
Basic Principles Observed and Reported. Lowest level of technology readiness. Scientific research begins to be translated into technology's basic properties.	*TRL 1 certification is not dependent on criteria. The Principal Investigator determines a TRL 1 with conceptualization.*	**Principal Investigator.**

TECHNOLOGY READINESS LEVEL 2 HARDWARE MATURITY CHECKLIST					
DoD TRL 2 Definition	**TRL 2 Hardware Maturity Criteria**	**Met[1]**	**Not Met[2]**	**N/A[3]**	**Certification Authority**
Technology Concept and/or Application Formulated Invention begins. Once Basic principles are observed, practical applications can be invented. The application is speculative and there is no proof or detailed analysis to support the assumption. Examples are still limited to paper studies.	1. Basic physical principles have been confirmed independently. Physical laws and assumptions used in new technologies defined. *Provide details.*	□	□	□	**Principal Investigator and MDA/DV Project Sponsor .**Certifies that technology has met all applicable TRL 2 Hardware Maturity Criteria and has thus achieved TRL 2 status.
	2. Basic elements of technology have been identified. *Provide a list of the elements of technology. Describe and compare relationship of old to new elements.*	□	□	□	
	3. An apparent theoretical or empirical design solution identified. *Describe design in as much detail as possible.*	□	□	□	
	4. Components of technology have been partially characterized. *Provide details on characterization for each component.*	□	□	□	
	5. Design techniques/codes have been identified/developed and performance predictions made for each element. *Provide details on design techniques/code and predictions made.*	□	□	□	
	6. Potential BMDS application(s) have been identified. *Provide a discussion of each of these applications.*	□	□	□	
1. For each criterion that HAS been met provide relevant background information for verification as noted. 2. For each criterion that HAS NOT been met provide the status and an estimate when the criteria will be met. 3. For each criterion marked N/A provide supporting documentation for this selection.					

TECHNOLOGY READINESS LEVEL 3
HARDWARE MATURITY CHECKLIST

DoD TRL 3 Definition	TRL 3 Hardware Maturity Criteria	Met[1]	Not Met[2]	N/A[3]	Certification Authority
Analytical and Experimental Critical Function and/or Characteristic Proof of Concept. Active research and development is initiated. This includes analytical studies and laboratory studies to physically validate analytical predictions of separate elements of the technology. Examples include components that are not yet integrated or representative.	1. Performance predictions of elements of technology capability validated by: a. Analytical Studies, b. Laboratory Experiments, and/or c. Modeling and Simulation *Provide details of the studies, experiments, and M&S.*	□ □ □	□ □ □	□ □ □	**Principal Investigator and MDA/DV Project Sponsor in consultation with potential End Users(s).** Certifies that technology has met all applicable TRL 3 Hardware Maturity Criteria and has thus achieved TRL 3 status.
	2. Scaling studies have been started. *Define the goals of the studies and how the goals relate to the BMDS mission.*	□	□	□	
	3. Preliminary performance characteristics and measures have been identified and estimated. *Quantify level of performance.*	□	□	□	
	4. Cross technology effects *(if any)* have begun to be identified. *Identify other new or in development technology that could increase performance and reduce risk.*	□	□	□	
	5. Design techniques/codes have been identified and defined to the point where small applications may be analyzed/simulated. *Provide details.*	□	□	□	

1. For each criterion that HAS been met provide relevant background information for verification as noted.
2. For each criterion that HAS NOT been met provide the status and an estimate when the criteria will be met.
3. For each criterion marked N/A provide supporting documentation for this selection.

TECHNOLOGY READINESS LEVEL 4
HARDWARE MATURITY CHECKLIST

DoD TRL 4 Definition	TRL 4 Hardware Maturity Criteria	Met[1]	Not Met[2]	N/A[3]	Certification Authority
Component and/or Breadboard Validation in Laboratory Environment. Basic technological components are integrated to establish that the pieces will work	1. Low fidelity hardware technology "system" integration and engineering completed in a lab environment with hardware in the loop/computer in the loop tools to establish component compatibility. *Provide summary reports of efforts including results.*	□	□	□	**Deputy for DV in consultation with MDA/DV Project Sponsor, SE, and potential End**
	2. Technology demonstrates basic functionality in simplified environment. *Describe demonstrated functionality and provide summary of collected data.*	□	□	□	

TECHNOLOGY READINESS LEVEL 4 **HARDWARE MATURITY CHECKLIST**					
DoD TRL 4 Definition	**TRL 4 Hardware Maturity Criteria**	**Met[1]**	**Not Met[2]**	**N/A[3]**	**Certification Authority**
together. This is relatively "low fidelity" compared to the eventual system. Examples include integration of "ad hoc" hardware in a laboratory.	3. Scaling studies have continued to next higher assembly from previous assessment. a. Scaling documents and diagrams of technology have been completed. b. Scalable technology prototypes have been produced. *BMDS mission enhancement(s) clearly defined within goals of the study.*	□ □	□ □	□ □	**Users(s); ATC Secretariat informed.** Certifies that technology has met all applicable TRL 4 Hardware Maturity Criteria and has thus achieved TRL 4 status.
	4. Integration studies have been started. *Provide a ROM integration cost estimate, with Systems Engineering, System Executive Officer, and end user inputs and coordination.*	□	□	□	
	5. Draft conceptual hardware and software designs have been documented. *Provide copy of documentation.*	□	□	□	
	6. Some software components are available. Executables are debugged, compiled and expert programmer is able to execute. *Provide documentation of efforts.*	□	□	□	
	7. Piece parts and components in a pre-production form exist. *Provide documentation of efforts.*	□	□	□	
	8. Production and integration planning have begun. *Document planning efforts.*	□	□	□	
	9. Performance metrics have been established. *Provide performance metrics.*	□	□	□	
	10. Cross technology issues *(if any)* have been fully identified. *Document issues.*	□	□	□	
	11. Design techniques/codes have been defined to the point where medium level problems may be accommodated. *Document level of fidelity and ownership of codes.*	□	□	□	
	12. Begin discussions/negotiations of Technology Transition Agreement to include data in items 1 through 5, 8, and 9.	□	□	□	
1. For each criterion that HAS been met provide relevant background information for verification as noted. **2. For each criterion that HAS NOT been met provide the status and an estimate when the criteria will be met.** **3. For each criterion marked N/A provide supporting documentation for this selection**					

TECHNOLOGY READINESS LEVEL 5 HARDWARE MATURITY CHECKLIST					
DoD TRL 5 Definition	**TRL 5 Hardware Maturity Criteria**	**Met[1]**	**Not Met[2]**	**N/A[3]**	**Certification Authority**
Component and/or Breadboard Validation in Relevant Environment. Fidelity of breadboard technology increases significantly. The basic technological components are integrated with reasonably realistic supporting elements so that the technology can be tested in simulated environment. Examples include "high fidelity" laboratory integration of components.	1. High fidelity lab integration of the hardware technology "system" completed and ready for testing in realistic simulated environments. *Provide summary reports of integration efforts including results. Define relevant environment used in testing.*	□	□	□	**Deputy for DV, Deputy for SE, and End User Deputy(ies) in consultation with Deputy for MP and Deputy Director for Technology and Engineering; ATC Secretariate informed.** Certify that technology has met all applicable TRL 5 Hardware Maturity Criteria and has thus achieved TRL 5 status.
	2. Preliminary hardware technology ""engineering report completed that addresses: a. Performance (including how measured performance translates to expected performance of final product) b. Integration c. Test and Evaluation d. Mechanical and Electrical Interfaces *Provide preliminary* hardware technology *"system" engineering report.*	□ □ □ □	□ □ □ □	□ □ □ □	
	3. Detailed design drawings have been completed. Three view drawings and wiring diagrams have been submitted.	□	□	□	
	4. Pre-production hardware available. a. Prototypes have been created. b. Production processes have been reviewed with MDA/MP. *Update ROM integration cost estimate and provide first order schedule for integration with end user(s).*	□ □	□ □	□ □	
	5. Form, fit, and function for application has begun to be addressed in conjunction with end user development staff. *Provide details of efforts to date.*	□	□	□	
	6. Cross technology effects *(if any)* identified and established through analysis. *Provide documentation of effects.*	□	□	□	
	7. Design techniques/codes have been defined to the point where largest problems defined. *Provide details on how this technology will solve largest problems.*	□	□	□	
	8. Scaling studies have continued to next higher assembly from previous assessment. *Describe scaling to new functional capability and regions of operational area.*	□	□	□	
	9. Technology Transition Agreement has been updated to reflect data in items 1 through 3, 5, and 8. TTA has been coordinated and approved by ATC or end user Deputy(ies) and Deputy for DV following approval at CCB.	□	□	□	

TECHNOLOGY READINESS LEVEL 5 **HARDWARE MATURITY CHECKLIST**					
DoD TRL 5 Definition	**TRL 5 Hardware Maturity Criteria**	**Met[1]**	**Not Met[2]**	**N/A[3]**	**Certification Authority**
1. For each criterion that HAS been met provide relevant background information for verification as noted. **2. For each criterion that HAS NOT been met provide the status and an estimate when the criteria will be met.** **3. For each criterion marked N/A provide supporting documentation for this selection.**					

TECHNOLOGY READINESS LEVEL 6 **HARDWARE MATURITY CHECKLIST**					
DoD TRL 6 Definition	**TRL 6 Hardware Maturity Criteria**	**Met[1]**	**Not Met[2]**	**N/A[3]**	**Certification Authority**
System/Subsystem Model or Prototype Demonstration in a Relevant Environment. Representative model or prototype system, which is well beyond the breadboard tested for level 5, is tested in a relevant environment. Represents a major step up in a technology's demonstrated readiness. Examples include testing a prototype in a high-fidelity laboratory environment or in simulated operational environment.	1. Materials, process, design, and integration methods have been employed. *Provide documentation of process, design, and integration methodology compliance with MDA Quality Assurance Plan.*	□	□	□	**Deputy for DV, Deputy for SE, and End User Deputy(ies) through MDA/DB and in consultation with Deputy for MP, Deputy Director for Technology and Engineering; ATC Secretariate informed.** Certifies that technology has met all applicable TRL 6 Hardware Maturity Criteria and has thus achieved TRL 6 status.
	2. Scaling issues that remain are identified and supporting analysis is complete. *Provide description of issues and resolution.*	□	□	□	
	3. Production demonstrations are complete. Production issues have been identified and major ones have been resolved. *Provide documentation of data, issues and resolutions.*	□	□	□	
	4. Some associated "Beta" version software is available.	□	□	□	
	5. Most pre-production hardware is available. *Provide documentation of identified shortfalls to end user(s) and/or testing organization.*	□	□	□	
	6. Draft production planning has been reviewed by end user and developer. *Update ROM integration cost estimate and update integration schedule with end user(s), MDA/SE, MDA/PI and MDA/MP.*	□	□	□	
	7. Draft design drawings are nearly complete.	□	□	□	
	8. Integration demonstrations have been completed, including cross technology issue measurement and performance characteristic validations. *Verification report compiled and reviewed by system engineer and testing organization.*	□	□	□	
	9. Have begun to establish an interface control process. *Provide process documentation to system engineer for review.*	□	□	□	

TECHNOLOGY READINESS LEVEL 6
HARDWARE MATURITY CHECKLIST

DoD TRL 6 Definition	TRL 6 Hardware Maturity Criteria	Met[1]	Not Met[2]	N/A[3]	Certification Authority
	10. Collection of actual maintainability, reliability, and supportability data has been started. *Provide RAM data to system engineer.*	□	□	□	
	11. Representative model or prototype is successfully tested in a high- fidelity laboratory or simulated operational environment. *Provide performance estimate and verification of capability enhancement with data collected.*	□	□	□	
	12. Hardware technology “system” specification complete. *Submit h*ardware technology “*system” specification for approval.*	□	□	□	
	13. Technology Transition Agreement has been updated to reflect data in items 1 through 4, 7 through 9, 11 and 12. TTA has been coordinated and approved by ATC or end user Deputy(ies) and Deputy for DV following approval at CCB	□	□	□	

1. For each criterion that HAS been met provide relevant background information for verification as noted.
2. For each criterion that HAS NOT been met provide the status and an estimate when the criteria will be met.
3. For each criterion marked N/A provide supporting documentation for this selection.

TECHNOLOGY READINESS LEVEL 7
HARDWARE MATURITY CHECKLIST

DoD TRL 7 Definition	TRL 7 Hardware Maturity Criteria	Met[1]	Not Met[2]	N/A[3]	Certification Authority
System Prototype Demonstration in an Operational Environment. Prototype near or at planned operational system. Represents a major step up from level 6, requiring the demonstration of an actual system prototype in an operational environment. Examples include testing the prototype in a test bed aircraft.	1. Materials, processes, methods, and design techniques have been identified and are moderately developed and verified.	□	□	□	**Cognizant Development Deputy in conjunction with SE.** Certifies that technology has met all applicable TRL 7 Hardware Maturity Criteria and has thus achieved TRL 7 status.
	2. Scaling is complete.	□	□	□	
	3. Production planning is complete.	□	□	□	
	4. Pre-production hardware and software is available in limited quantities.	□	□	□	
	5. Draft design drawings are complete.	□	□	□	
	6. Maintainability, reliability, and supportability data growth is above 60% of total needed data.	□	□	□	
	7. Hardware technology “system” prototype successfully tested in a field environment.	□	□	□	

TECHNOLOGY READINESS LEVEL 7
HARDWARE MATURITY CHECKLIST

DoD TRL 7 Definition	TRL 7 Hardware Maturity Criteria	Met[1]	Not Met[2]	N/A[3]	Certification Authority

1. For each criterion that HAS been met provide relevant background information for verification as noted.
2. For each criterion that HAS NOT been met provide the status and an estimate when the criteria will be met.
3. For each criterion marked N/A provide supporting documentation for this selection.

TECHNOLOGY READINESS LEVEL 8
HARDWARE MATURITY CHECKLIST

DoD TRL 8 Definition	TRL 8 Hardware Maturity Criteria	Met[1]	Not Met[2]	N/A[3]	Certification Authority
Actual System Completed and Qualified Through Test and Demonstration. Technology has been proven to work in its final form and under expected conditions. In almost all cases, this level represents the end of true system development. Examples include developmental test and evaluation of the system in its intended weapon system to determine if it meets design specifications.	1. Interface control process has been completed and final architecture diagrams have been submitted.	□	□	□	**Cognizant Development Deputy in conjunction with SE.** Certifies that technology has met all applicable TRL 8 Hardware Maturity Criteria and has thus achieved TRL 8 status.
	2. Maintainability, reliability, and supportability data collection has been completed.	□	□	□	
	3. Hardware technology successfully completes developmental test and evaluation.	□	□	□	
	4. Hardware technology has been proven to work in its final form and under expected conditions.	□	□	□	
		□	□	□	
		□	□	□	
		□	□	□	
		□	□	□	
		□	□	□	

1. For each criterion that HAS been met provide relevant background information for verification as noted.
2. For each criterion that HAS NOT been met provide the status and an estimate when the criteria will be met.
3. For each criterion marked N/A provide supporting documentation for this selection.

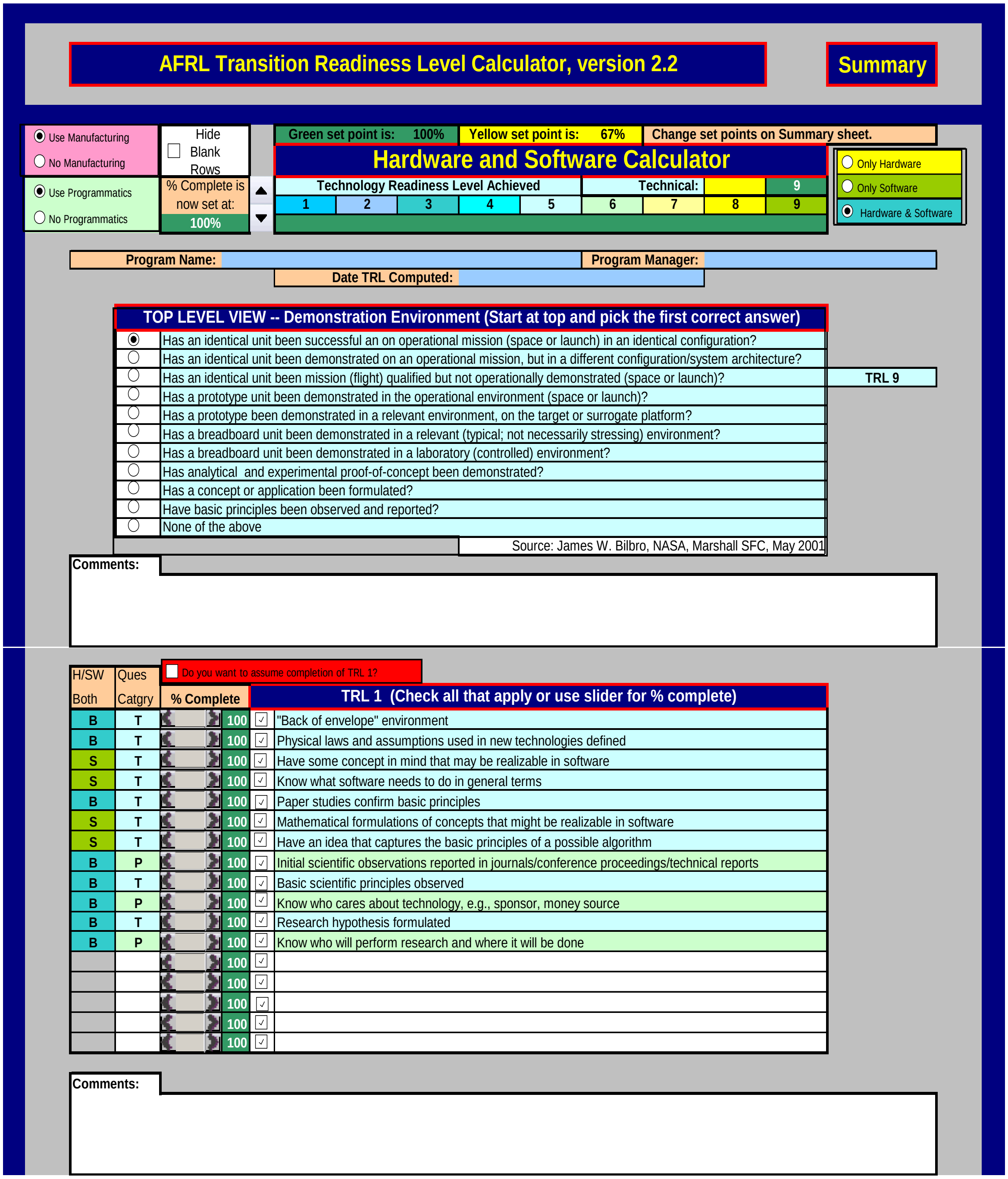
TECHNOLOGY READINESS LEVEL 9
HARDWARE MATURITY CHECKLIST

DoD TRL 9 Definition	TRL 9 Hardware Maturity Criteria	Met[1]	Not Met[2]	N/A[3]	Certification Authority
Actual System Proven Through Successful Mission Operation. Actual application of the	1. Hardware technology successfully completes operational test and evaluation.	□	□	□	**Cognizant Development Deputy in conjunction with SE.**
	2. Training Plan has been implemented.	□	□	□	
	3. Supportability Plan has been implemented	□	□	□	

TECHNOLOGY READINESS LEVEL 9 HARDWARE MATURITY CHECKLIST					
DoD TRL 9 Definition	**TRL 9 Hardware Maturity Criteria**	**Met[1]**	**Not Met[2]**	**N/A[3]**	**Certification Authority**
technology in its final form and under mission conditions, such as those encountered in operational test and evaluation. Examples include using the system under operational mission conditions.	4. Program Protection Plan has been implemented	□	□	□	Certifies that technology has met all applicable TRL 9 Hardware Maturity Criteria and has thus achieved TRL 9 status..
	5. Safety/Adverse effects issues have been identified and mitigated	□	□	□	
	6. Operational Concept has been implemented successfully	□	□	□	
		□	□	□	
		□	□	□	
		□	□	□	
1. For each criterion that HAS been met provide relevant background information for verification as noted. 2. For each criterion that HAS NOT been met provide the status and an estimate when the criteria will be met. 3. For each criterion marked N/A provide supporting documentation for this selection.					

Table 4. Missile Defense Agency Hardware Technology Readiness Level Checklist [From: Missile Defense Agency, 2007]

A Technology Readiness Calculator was developed by William Nolte who works for the Air Force Research Laboratory. It is available at the DoD Acquisition Community Connection website; Version 2.2 is available at https://acc.dau.mil/CommunityBrowser.aspx?id=25811&lang=en-US. It is a Microsoft Excel™ spreadsheet application with a standard set of questions about hardware, software, manufacturing, engineering artifacts, and the acquisition program. It calculates and graphically displays a TRL achieved. This calculator is unique in that it looks at technology holistically within the context of the software and hardware technology itself, manufacturing, system development and programmatics. See Figure 22 for the calculator. In discussion with the Institute of Defense Analyses which supports the Missile Defense Agency, they are looking into creating a TRL calculator as well.



AFRL Transition Readiness Level Calculator, version 2.2

Summary

● Use Manufacturing
○ No Manufacturing

● Use Programmatics
○ No Programmatics

Hide □ Blank Rows

% Complete is now set at: 100%

Green set point is: 100%	Yellow set point is: 67%	Change set points on Summary sheet.

Hardware and Software Calculator

Technology Readiness Level Achieved					Technical:			9
1	2	3	4	5	6	7	8	9

○ Only Hardware
○ Only Software
● Hardware & Software

Program Name:

Program Manager:

Date TRL Computed:

TOP LEVEL VIEW -- Demonstration Environment (Start at top and pick the first correct answer)

●	Has an identical unit been successful an on operational mission (space or launch) in an identical configuration?	
○	Has an identical unit been demonstrated on an operational mission, but in a different configuration/system architecture?	
○	Has an identical unit been mission (flight) qualified but not operationally demonstrated (space or launch)?	TRL 9
○	Has a prototype unit been demonstrated in the operational environment (space or launch)?	
○	Has a prototype been demonstrated in a relevant environment, on the target or surrogate platform?	
○	Has a breadboard unit been demonstrated in a relevant (typical; not necessarily stressing) environment?	
○	Has a breadboard unit been demonstrated in a laboratory (controlled) environment?	
○	Has analytical and experimental proof-of-concept been demonstrated?	
○	Has a concept or application been formulated?	
○	Have basic principles been observed and reported?	
○	None of the above	

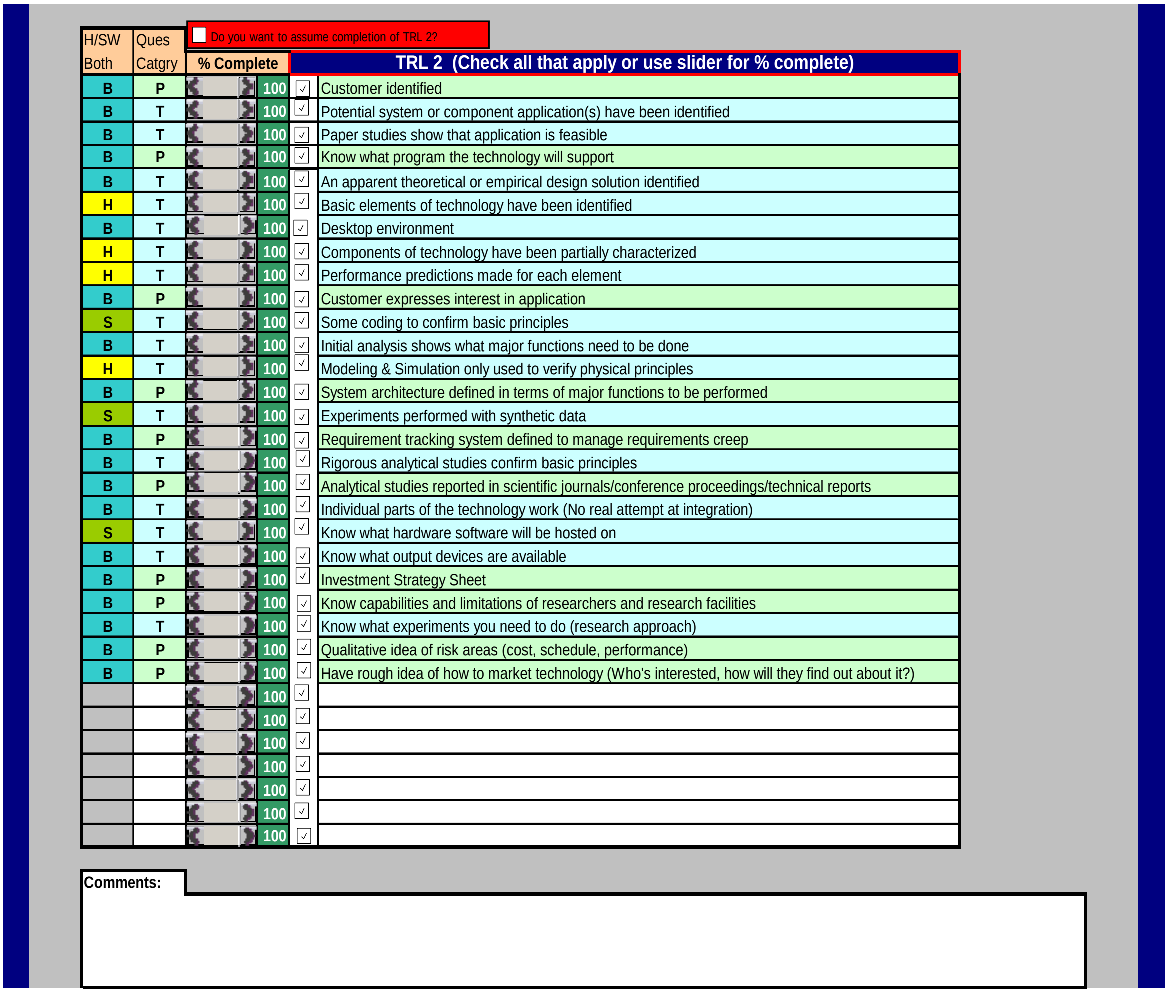
Source: James W. Bilbro, NASA, Marshall SFC, May 2001

Comments:

□ Do you want to assume completion of TRL 1?

H/SW Both	Ques Catgry	% Complete		TRL 1 (Check all that apply or use slider for % complete)
B	T	100	✓	"Back of envelope" environment
B	T	100	✓	Physical laws and assumptions used in new technologies defined
S	T	100	✓	Have some concept in mind that may be realizable in software
S	T	100	✓	Know what software needs to do in general terms
B	T	100	✓	Paper studies confirm basic principles
S	T	100	✓	Mathematical formulations of concepts that might be realizable in software
S	T	100	✓	Have an idea that captures the basic principles of a possible algorithm
B	P	100	✓	Initial scientific observations reported in journals/conference proceedings/technical reports
B	T	100	✓	Basic scientific principles observed
B	P	100	✓	Know who cares about technology, e.g., sponsor, money source
B	T	100	✓	Research hypothesis formulated
B	P	100	✓	Know who will perform research and where it will be done
		100	✓	
		100	✓	
		100	✓	
		100	✓	
		100	✓	

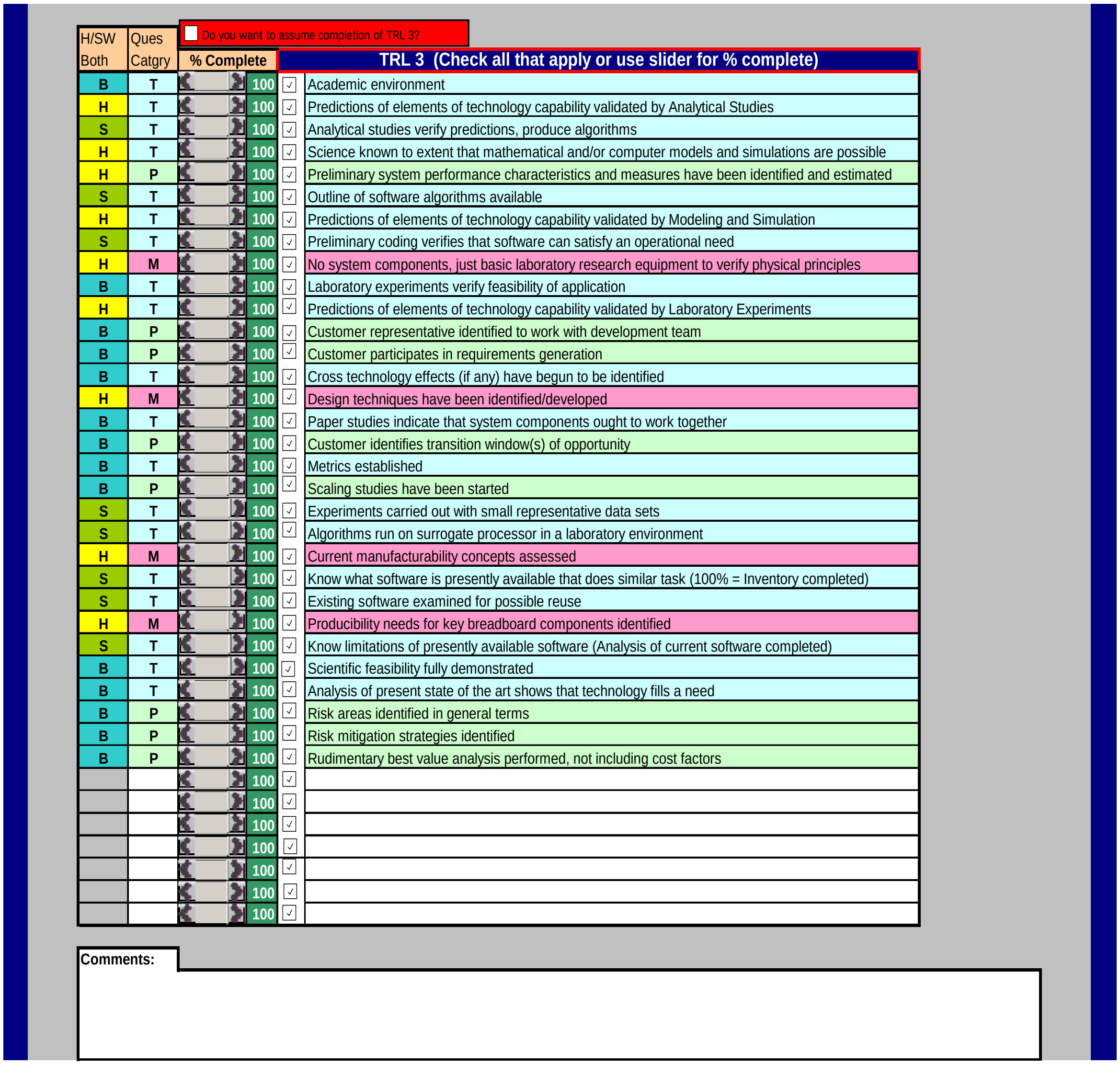
Comments:



□ Do you want to assume completion of TRL 2?

H/SW Both	Ques Catgry	% Complete		TRL 2 (Check all that apply or use slider for % complete)
B	P	100	☑	Customer identified
B	T	100	☑	Potential system or component application(s) have been identified
B	T	100	☑	Paper studies show that application is feasible
B	P	100	☑	Know what program the technology will support
B	T	100	☑	An apparent theoretical or empirical design solution identified
H	T	100	☑	Basic elements of technology have been identified
B	T	100	☑	Desktop environment
H	T	100	☑	Components of technology have been partially characterized
H	T	100	☑	Performance predictions made for each element
B	P	100	☑	Customer expresses interest in application
S	T	100	☑	Some coding to confirm basic principles
B	T	100	☑	Initial analysis shows what major functions need to be done
H	T	100	☑	Modeling & Simulation only used to verify physical principles
B	P	100	☑	System architecture defined in terms of major functions to be performed
S	T	100	☑	Experiments performed with synthetic data
B	P	100	☑	Requirement tracking system defined to manage requirements creep
B	T	100	☑	Rigorous analytical studies confirm basic principles
B	P	100	☑	Analytical studies reported in scientific journals/conference proceedings/technical reports
B	T	100	☑	Individual parts of the technology work (No real attempt at integration)
S	T	100	☑	Know what hardware software will be hosted on
B	T	100	☑	Know what output devices are available
B	P	100	☑	Investment Strategy Sheet
B	P	100	☑	Know capabilities and limitations of researchers and research facilities
B	T	100	☑	Know what experiments you need to do (research approach)
B	P	100	☑	Qualitative idea of risk areas (cost, schedule, performance)
B	P	100	☑	Have rough idea of how to market technology (Who's interested, how will they find out about it?)
		100	☑	
		100	☑	
		100	☑	
		100	☑	
		100	☑	
		100	☑	
		100	☑	

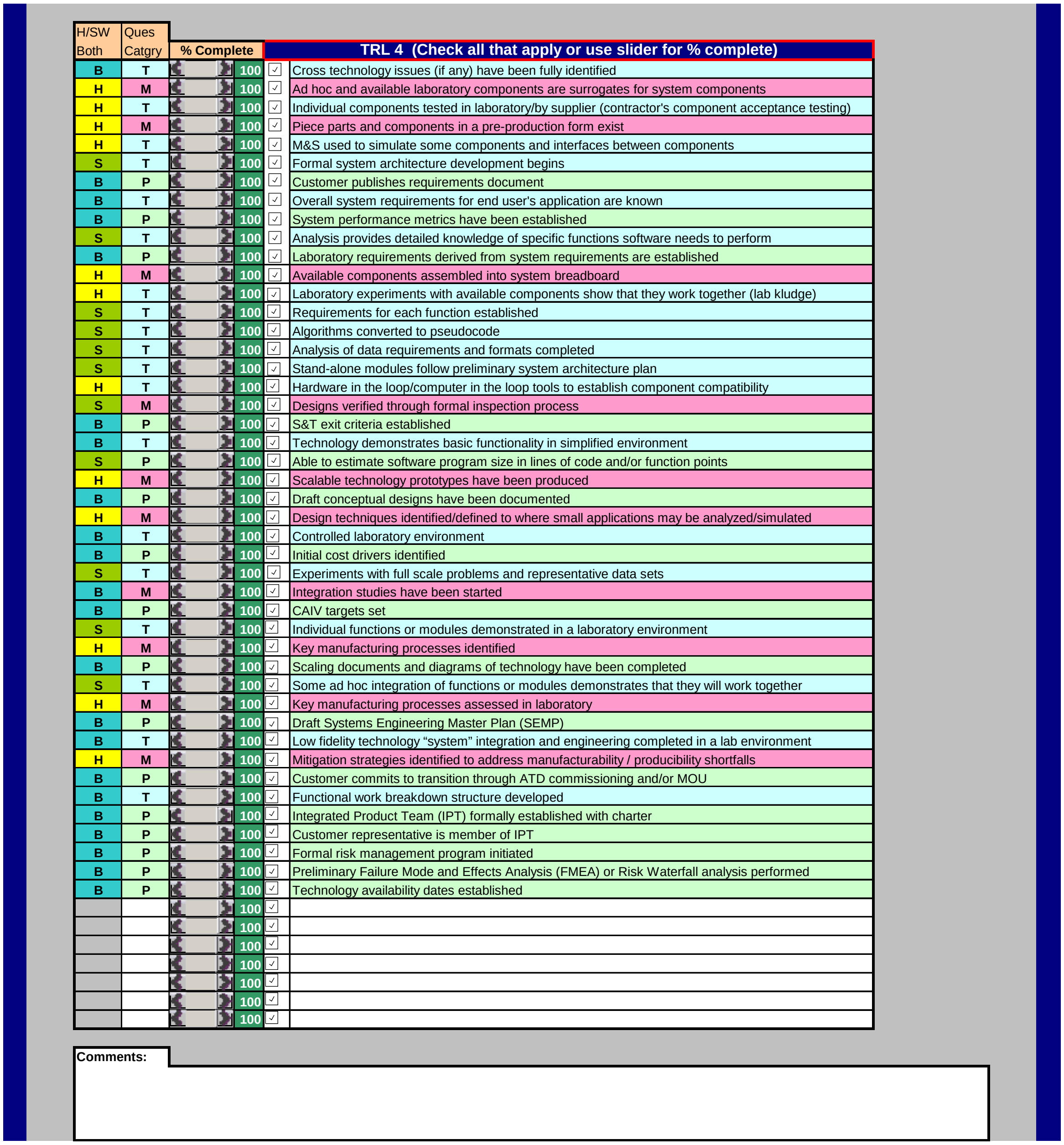
Comments:



☐ Do you want to assume completion of TRL 3?

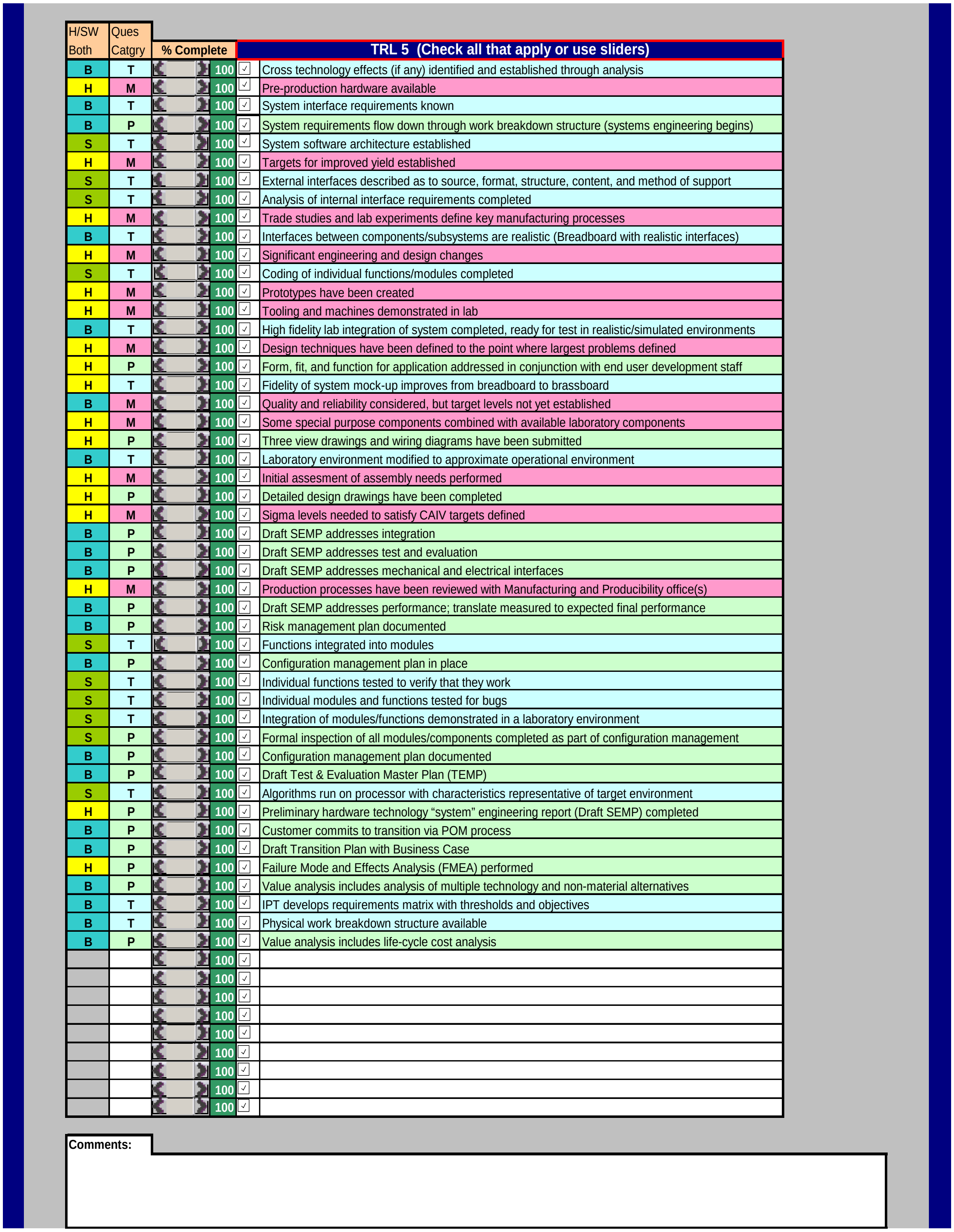
H/SW Both	Ques Catgry	% Complete		TRL 3 (Check all that apply or use slider for % complete)
B	T	100	☑	Academic environment
H	T	100	☑	Predictions of elements of technology capability validated by Analytical Studies
S	T	100	☑	Analytical studies verify predictions, produce algorithms
H	T	100	☑	Science known to extent that mathematical and/or computer models and simulations are possible
H	P	100	☑	Preliminary system performance characteristics and measures have been identified and estimated
S	T	100	☑	Outline of software algorithms available
H	T	100	☑	Predictions of elements of technology capability validated by Modeling and Simulation
S	T	100	☑	Preliminary coding verifies that software can satisfy an operational need
H	M	100	☑	No system components, just basic laboratory research equipment to verify physical principles
B	T	100	☑	Laboratory experiments verify feasibility of application
H	T	100	☑	Predictions of elements of technology capability validated by Laboratory Experiments
B	P	100	☑	Customer representative identified to work with development team
B	P	100	☑	Customer participates in requirements generation
B	T	100	☑	Cross technology effects (if any) have begun to be identified
H	M	100	☑	Design techniques have been identified/developed
B	T	100	☑	Paper studies indicate that system components ought to work together
B	P	100	☑	Customer identifies transition window(s) of opportunity
B	T	100	☑	Metrics established
B	P	100	☑	Scaling studies have been started
S	T	100	☑	Experiments carried out with small representative data sets
S	T	100	☑	Algorithms run on surrogate processor in a laboratory environment
H	M	100	☑	Current manufacturability concepts assessed
S	T	100	☑	Know what software is presently available that does similar task (100% = Inventory completed)
S	T	100	☑	Existing software examined for possible reuse
H	M	100	☑	Producibility needs for key breadboard components identified
S	T	100	☑	Know limitations of presently available software (Analysis of current software completed)
B	T	100	☑	Scientific feasibility fully demonstrated
B	T	100	☑	Analysis of present state of the art shows that technology fills a need
B	P	100	☑	Risk areas identified in general terms
B	P	100	☑	Risk mitigation strategies identified
B	P	100	☑	Rudimentary best value analysis performed, not including cost factors
		100	☑	
		100	☑	
		100	☑	
		100	☑	
		100	☑	
		100	☑	
		100	☑	

Comments:



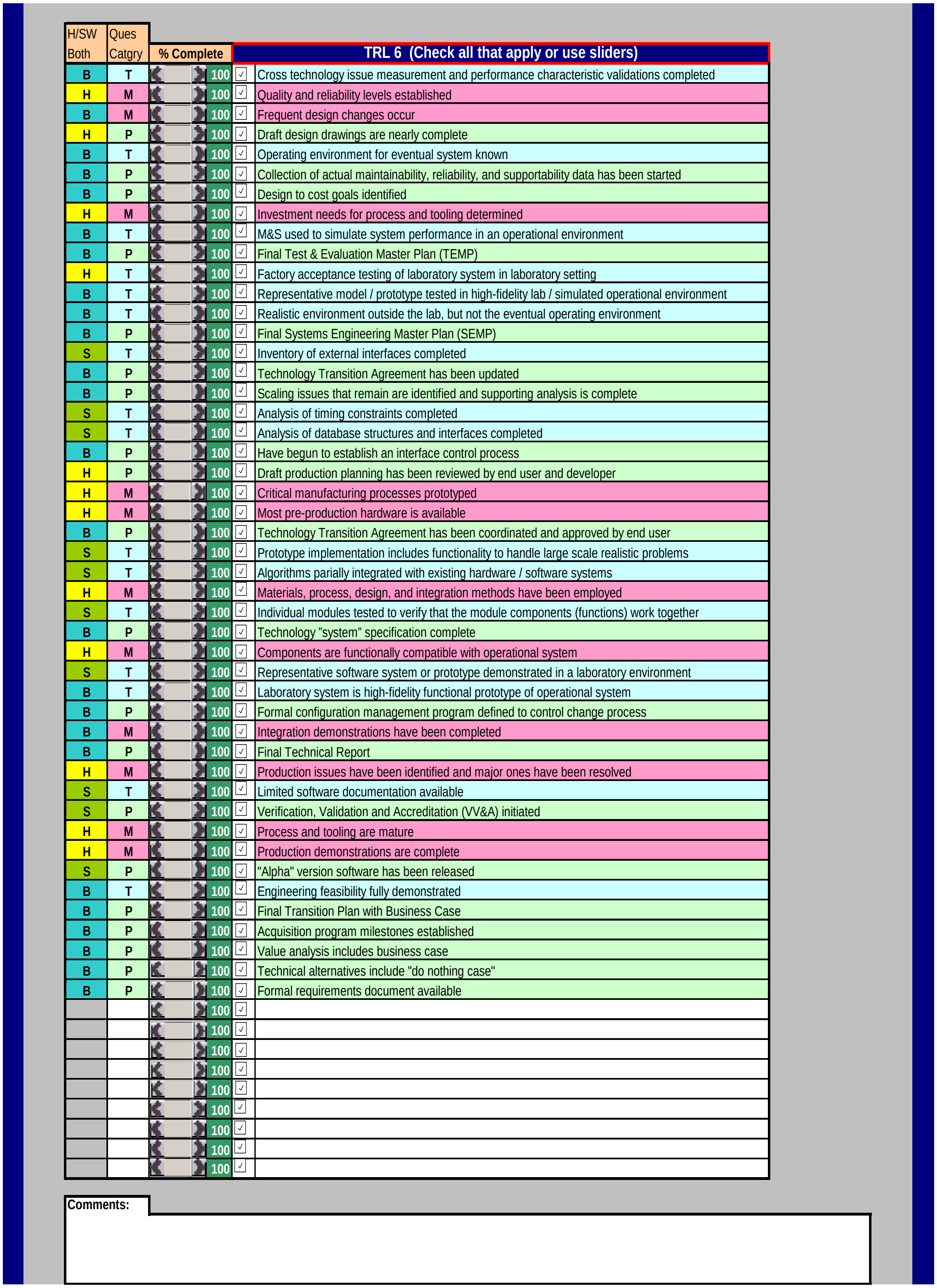
H/SW Both	Ques Catgry	% Complete		TRL 4 (Check all that apply or use slider for % complete)
B	T	100	☑	Cross technology issues (if any) have been fully identified
H	M	100	☑	Ad hoc and available laboratory components are surrogates for system components
H	T	100	☑	Individual components tested in laboratory/by supplier (contractor's component acceptance testing)
H	M	100	☑	Piece parts and components in a pre-production form exist
H	T	100	☑	M&S used to simulate some components and interfaces between components
S	T	100	☑	Formal system architecture development begins
B	P	100	☑	Customer publishes requirements document
B	T	100	☑	Overall system requirements for end user's application are known
B	P	100	☑	System performance metrics have been established
S	T	100	☑	Analysis provides detailed knowledge of specific functions software needs to perform
B	P	100	☑	Laboratory requirements derived from system requirements are established
H	M	100	☑	Available components assembled into system breadboard
H	T	100	☑	Laboratory experiments with available components show that they work together (lab kludge)
S	T	100	☑	Requirements for each function established
S	T	100	☑	Algorithms converted to pseudocode
S	T	100	☑	Analysis of data requirements and formats completed
S	T	100	☑	Stand-alone modules follow preliminary system architecture plan
H	T	100	☑	Hardware in the loop/computer in the loop tools to establish component compatibility
S	M	100	☑	Designs verified through formal inspection process
B	P	100	☑	S&T exit criteria established
B	T	100	☑	Technology demonstrates basic functionality in simplified environment
S	P	100	☑	Able to estimate software program size in lines of code and/or function points
H	M	100	☑	Scalable technology prototypes have been produced
B	P	100	☑	Draft conceptual designs have been documented
H	M	100	☑	Design techniques identified/defined to where small applications may be analyzed/simulated
B	T	100	☑	Controlled laboratory environment
B	P	100	☑	Initial cost drivers identified
S	T	100	☑	Experiments with full scale problems and representative data sets
B	M	100	☑	Integration studies have been started
B	P	100	☑	CAIV targets set
S	T	100	☑	Individual functions or modules demonstrated in a laboratory environment
H	M	100	☑	Key manufacturing processes identified
B	P	100	☑	Scaling documents and diagrams of technology have been completed
S	T	100	☑	Some ad hoc integration of functions or modules demonstrates that they will work together
H	M	100	☑	Key manufacturing processes assessed in laboratory
B	P	100	☑	Draft Systems Engineering Master Plan (SEMP)
B	T	100	☑	Low fidelity technology “system” integration and engineering completed in a lab environment
H	M	100	☑	Mitigation strategies identified to address manufacturability / producibility shortfalls
B	P	100	☑	Customer commits to transition through ATD commissioning and/or MOU
B	T	100	☑	Functional work breakdown structure developed
B	P	100	☑	Integrated Product Team (IPT) formally established with charter
B	P	100	☑	Customer representative is member of IPT
B	P	100	☑	Formal risk management program initiated
B	P	100	☑	Preliminary Failure Mode and Effects Analysis (FMEA) or Risk Waterfall analysis performed
B	P	100	☑	Technology availability dates established
		100	☑	
		100	☑	
		100	☑	
		100	☑	
		100	☑	
		100	☑	
		100	☑	

Comments:



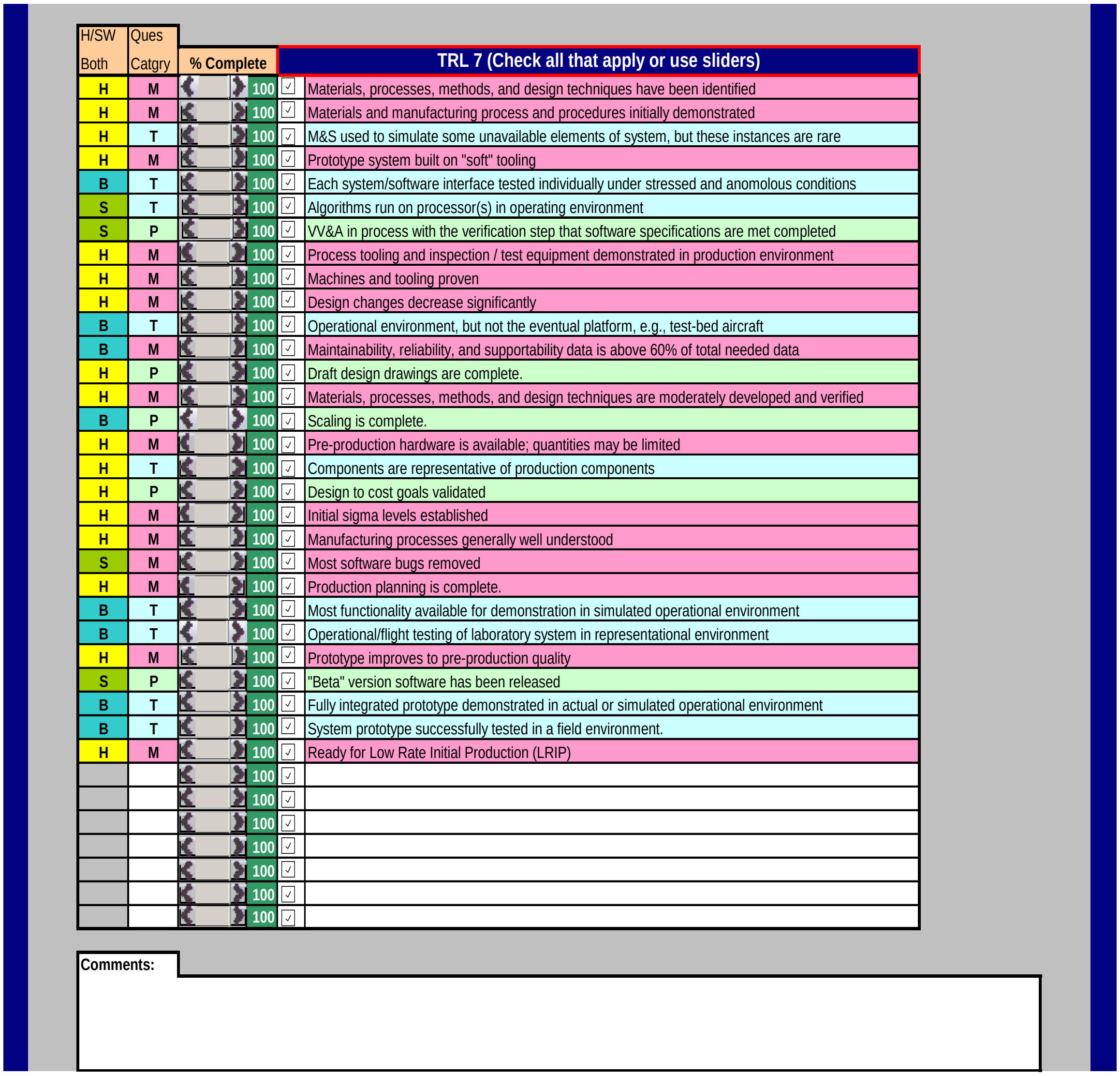
H/SW	Ques			
Both	Catgry	% Complete		TRL 5 (Check all that apply or use sliders)
B	T	100	☑	Cross technology effects (if any) identified and established through analysis
H	M	100	☑	Pre-production hardware available
B	T	100	☑	System interface requirements known
B	P	100	☑	System requirements flow down through work breakdown structure (systems engineering begins)
S	T	100	☑	System software architecture established
H	M	100	☑	Targets for improved yield established
S	T	100	☑	External interfaces described as to source, format, structure, content, and method of support
S	T	100	☑	Analysis of internal interface requirements completed
H	M	100	☑	Trade studies and lab experiments define key manufacturing processes
B	T	100	☑	Interfaces between components/subsystems are realistic (Breadboard with realistic interfaces)
H	M	100	☑	Significant engineering and design changes
S	T	100	☑	Coding of individual functions/modules completed
H	M	100	☑	Prototypes have been created
H	M	100	☑	Tooling and machines demonstrated in lab
B	T	100	☑	High fidelity lab integration of system completed, ready for test in realistic/simulated environments
H	M	100	☑	Design techniques have been defined to the point where largest problems defined
H	P	100	☑	Form, fit, and function for application addressed in conjunction with end user development staff
H	T	100	☑	Fidelity of system mock-up improves from breadboard to brassboard
B	M	100	☑	Quality and reliability considered, but target levels not yet established
H	M	100	☑	Some special purpose components combined with available laboratory components
H	P	100	☑	Three view drawings and wiring diagrams have been submitted
B	T	100	☑	Laboratory environment modified to approximate operational environment
H	M	100	☑	Initial assesment of assembly needs performed
H	P	100	☑	Detailed design drawings have been completed
H	M	100	☑	Sigma levels needed to satisfy CAIV targets defined
B	P	100	☑	Draft SEMP addresses integration
B	P	100	☑	Draft SEMP addresses test and evaluation
B	P	100	☑	Draft SEMP addresses mechanical and electrical interfaces
H	M	100	☑	Production processes have been reviewed with Manufacturing and Producibility office(s)
B	P	100	☑	Draft SEMP addresses performance; translate measured to expected final performance
B	P	100	☑	Risk management plan documented
S	T	100	☑	Functions integrated into modules
B	P	100	☑	Configuration management plan in place
S	T	100	☑	Individual functions tested to verify that they work
S	T	100	☑	Individual modules and functions tested for bugs
S	T	100	☑	Integration of modules/functions demonstrated in a laboratory environment
S	P	100	☑	Formal inspection of all modules/components completed as part of configuration management
B	P	100	☑	Configuration management plan documented
B	P	100	☑	Draft Test & Evaluation Master Plan (TEMP)
S	T	100	☑	Algorithms run on processor with characteristics representative of target environment
H	P	100	☑	Preliminary hardware technology “system” engineering report (Draft SEMP) completed
B	P	100	☑	Customer commits to transition via POM process
B	P	100	☑	Draft Transition Plan with Business Case
H	P	100	☑	Failure Mode and Effects Analysis (FMEA) performed
B	P	100	☑	Value analysis includes analysis of multiple technology and non-material alternatives
B	T	100	☑	IPT develops requirements matrix with thresholds and objectives
B	T	100	☑	Physical work breakdown structure available
B	P	100	☑	Value analysis includes life-cycle cost analysis
		100	☑	
		100	☑	
		100	☑	
		100	☑	
		100	☑	
		100	☑	
		100	☑	
		100	☑	
		100	☑	

Comments:



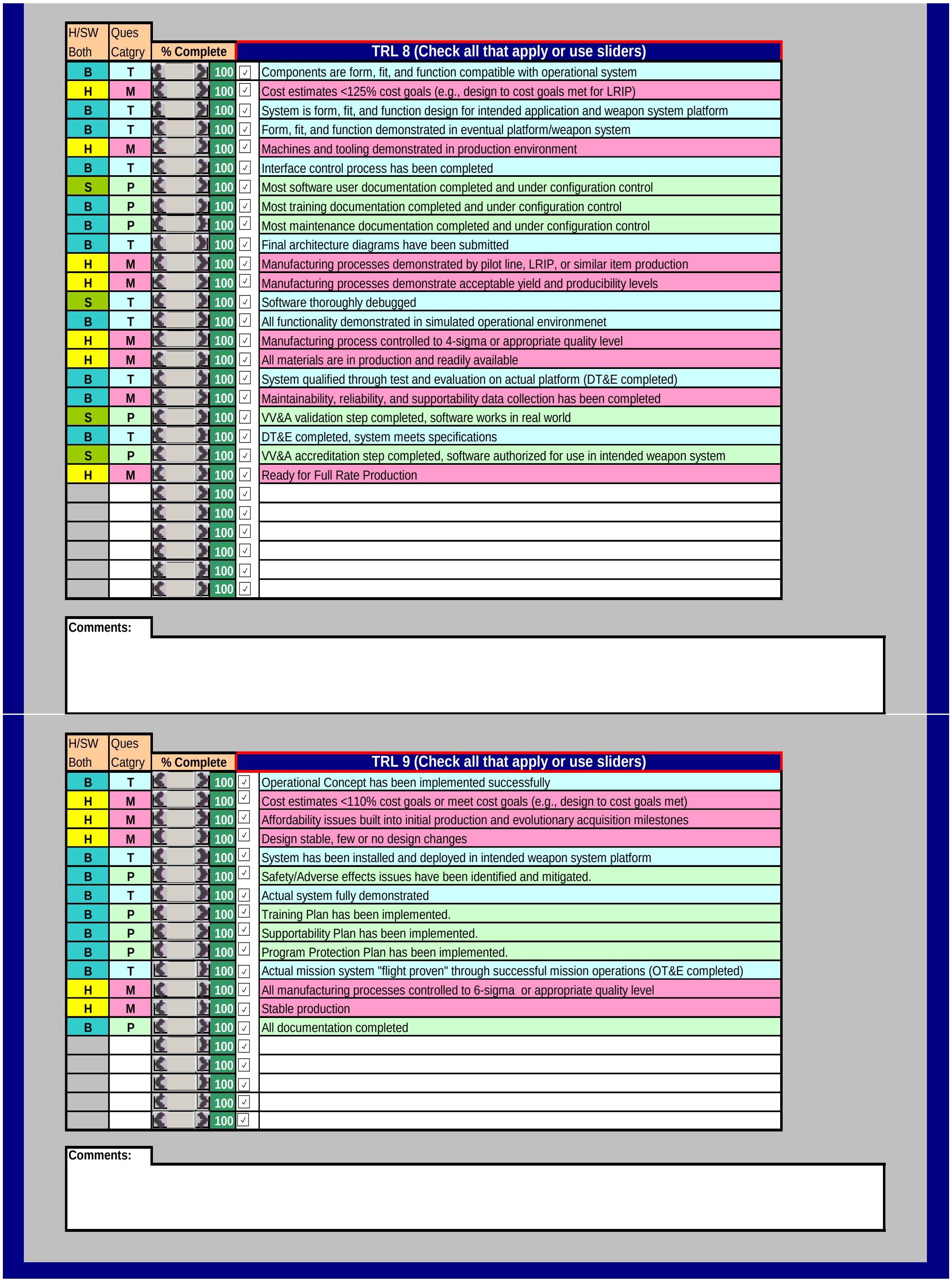
H/SW Both	Ques Catgry	% Complete		TRL 6 (Check all that apply or use sliders)
B	T	100	☑	Cross technology issue measurement and performance characteristic validations completed
H	M	100	☑	Quality and reliability levels established
B	M	100	☑	Frequent design changes occur
H	P	100	☑	Draft design drawings are nearly complete
B	T	100	☑	Operating environment for eventual system known
B	P	100	☑	Collection of actual maintainability, reliability, and supportability data has been started
B	P	100	☑	Design to cost goals identified
H	M	100	☑	Investment needs for process and tooling determined
B	T	100	☑	M&S used to simulate system performance in an operational environment
B	P	100	☑	Final Test & Evaluation Master Plan (TEMP)
H	T	100	☑	Factory acceptance testing of laboratory system in laboratory setting
B	T	100	☑	Representative model / prototype tested in high-fidelity lab / simulated operational environment
B	T	100	☑	Realistic environment outside the lab, but not the eventual operating environment
B	P	100	☑	Final Systems Engineering Master Plan (SEMP)
S	T	100	☑	Inventory of external interfaces completed
B	P	100	☑	Technology Transition Agreement has been updated
B	P	100	☑	Scaling issues that remain are identified and supporting analysis is complete
S	T	100	☑	Analysis of timing constraints completed
S	T	100	☑	Analysis of database structures and interfaces completed
B	P	100	☑	Have begun to establish an interface control process
H	P	100	☑	Draft production planning has been reviewed by end user and developer
H	M	100	☑	Critical manufacturing processes prototyped
H	M	100	☑	Most pre-production hardware is available
B	P	100	☑	Technology Transition Agreement has been coordinated and approved by end user
S	T	100	☑	Prototype implementation includes functionality to handle large scale realistic problems
S	T	100	☑	Algorithms parially integrated with existing hardware / software systems
H	M	100	☑	Materials, process, design, and integration methods have been employed
S	T	100	☑	Individual modules tested to verify that the module components (functions) work together
B	P	100	☑	Technology ”system” specification complete
H	M	100	☑	Components are functionally compatible with operational system
S	T	100	☑	Representative software system or prototype demonstrated in a laboratory environment
B	T	100	☑	Laboratory system is high-fidelity functional prototype of operational system
B	P	100	☑	Formal configuration management program defined to control change process
B	M	100	☑	Integration demonstrations have been completed
B	P	100	☑	Final Technical Report
H	M	100	☑	Production issues have been identified and major ones have been resolved
S	T	100	☑	Limited software documentation available
S	P	100	☑	Verification, Validation and Accreditation (VV&A) initiated
H	M	100	☑	Process and tooling are mature
H	M	100	☑	Production demonstrations are complete
S	P	100	☑	"Alpha" version software has been released
B	T	100	☑	Engineering feasibility fully demonstrated
B	P	100	☑	Final Transition Plan with Business Case
B	P	100	☑	Acquisition program milestones established
B	P	100	☑	Value analysis includes business case
B	P	100	☑	Technical alternatives include "do nothing case"
B	P	100	☑	Formal requirements document available
		100	☑	
		100	☑	
		100	☑	
		100	☑	
		100	☑	
		100	☑	
		100	☑	
		100	☑	
		100	☑	

Comments:



H/SW Both	Ques Catgry	% Complete		TRL 7 (Check all that apply or use sliders)
H	M	100	☑	Materials, processes, methods, and design techniques have been identified
H	M	100	☑	Materials and manufacturing process and procedures initially demonstrated
H	T	100	☑	M&S used to simulate some unavailable elements of system, but these instances are rare
H	M	100	☑	Prototype system built on "soft" tooling
B	T	100	☑	Each system/software interface tested individually under stressed and anomolous conditions
S	T	100	☑	Algorithms run on processor(s) in operating environment
S	P	100	☑	VV&A in process with the verification step that software specifications are met completed
H	M	100	☑	Process tooling and inspection / test equipment demonstrated in production environment
H	M	100	☑	Machines and tooling proven
H	M	100	☑	Design changes decrease significantly
B	T	100	☑	Operational environment, but not the eventual platform, e.g., test-bed aircraft
B	M	100	☑	Maintainability, reliability, and supportability data is above 60% of total needed data
H	P	100	☑	Draft design drawings are complete.
H	M	100	☑	Materials, processes, methods, and design techniques are moderately developed and verified
B	P	100	☑	Scaling is complete.
H	M	100	☑	Pre-production hardware is available; quantities may be limited
H	T	100	☑	Components are representative of production components
H	P	100	☑	Design to cost goals validated
H	M	100	☑	Initial sigma levels established
H	M	100	☑	Manufacturing processes generally well understood
S	M	100	☑	Most software bugs removed
H	M	100	☑	Production planning is complete.
B	T	100	☑	Most functionality available for demonstration in simulated operational environment
B	T	100	☑	Operational/flight testing of laboratory system in representational environment
H	M	100	☑	Prototype improves to pre-production quality
S	P	100	☑	"Beta" version software has been released
B	T	100	☑	Fully integrated prototype demonstrated in actual or simulated operational environment
B	T	100	☑	System prototype successfully tested in a field environment.
H	M	100	☑	Ready for Low Rate Initial Production (LRIP)
		100	☑	
		100	☑	
		100	☑	
		100	☑	
		100	☑	
		100	☑	
		100	☑	

Comments:



H/SW Both	Ques Catgry	% Complete	TRL 8 (Check all that apply or use sliders)	
B	T	100	☑	Components are form, fit, and function compatible with operational system
H	M	100	☑	Cost estimates <125% cost goals (e.g., design to cost goals met for LRIP)
B	T	100	☑	System is form, fit, and function design for intended application and weapon system platform
B	T	100	☑	Form, fit, and function demonstrated in eventual platform/weapon system
H	M	100	☑	Machines and tooling demonstrated in production environment
B	T	100	☑	Interface control process has been completed
S	P	100	☑	Most software user documentation completed and under configuration control
B	P	100	☑	Most training documentation completed and under configuration control
B	P	100	☑	Most maintenance documentation completed and under configuration control
B	T	100	☑	Final architecture diagrams have been submitted
H	M	100	☑	Manufacturing processes demonstrated by pilot line, LRIP, or similar item production
H	M	100	☑	Manufacturing processes demonstrate acceptable yield and producibility levels
S	T	100	☑	Software thoroughly debugged
B	T	100	☑	All functionality demonstrated in simulated operational environmenet
H	M	100	☑	Manufacturing process controlled to 4-sigma or appropriate quality level
H	M	100	☑	All materials are in production and readily available
B	T	100	☑	System qualified through test and evaluation on actual platform (DT&E completed)
B	M	100	☑	Maintainability, reliability, and supportability data collection has been completed
S	P	100	☑	VV&A validation step completed, software works in real world
B	T	100	☑	DT&E completed, system meets specifications
S	P	100	☑	VV&A accreditation step completed, software authorized for use in intended weapon system
H	M	100	☑	Ready for Full Rate Production
		100	☑	
		100	☑	
		100	☑	
		100	☑	
		100	☑	
		100	☑	

Comments:

H/SW Both	Ques Catgry	% Complete	TRL 9 (Check all that apply or use sliders)	
B	T	100	☑	Operational Concept has been implemented successfully
H	M	100	☑	Cost estimates <110% cost goals or meet cost goals (e.g., design to cost goals met)
H	M	100	☑	Affordability issues built into initial production and evolutionary acquisition milestones
H	M	100	☑	Design stable, few or no design changes
B	T	100	☑	System has been installed and deployed in intended weapon system platform
B	P	100	☑	Safety/Adverse effects issues have been identified and mitigated.
B	T	100	☑	Actual system fully demonstrated
B	P	100	☑	Training Plan has been implemented.
B	P	100	☑	Supportability Plan has been implemented.
B	P	100	☑	Program Protection Plan has been implemented.
B	T	100	☑	Actual mission system "flight proven" through successful mission operations (OT&E completed)
H	M	100	☑	All manufacturing processes controlled to 6-sigma or appropriate quality level
H	M	100	☑	Stable production
B	P	100	☑	All documentation completed
		100	☑	
		100	☑	
		100	☑	
		100	☑	
		100	☑	

Comments:

Figure 21. AFRL Nolte TRL Calculator v2.2 [From: Nolte, 2004]

H – Hardware	M – Manufacturing	T - Technical
S – Software	B – Both H and S	P – Programmatics

The GAO assesses DoD programs on a regular basis. Their findings consistently find programs using immature technologies sometimes through MS C. In one report of many, GAO-05-301 Defense Acquisitions: Assessments of Selected Major Weapons Programs, March 31, 2005 (GAO, 2005) had the following summary of a review of 54 DoD programs:

- Only 15% of programs began System Design and Development (SDD) with mature technology (TRL 7)
- Programs that started with mature technologies averaged 9% cost growth and a 7 month schedule delay; Programs that did not have mature technologies averaged 41% cost growth and a 13 month schedule delay
- At critical design review, 42% of programs demonstrated design stability (90% drawings releasable); Design stability not achievable with immature technologies
- Programs with stable designs at CDR averaged 6% cost growth; Programs without stable designs at CDR averaged 46% cost growth and a 29 month schedule delay

Given the track record of DoD programs selecting immature technologies, Congress passed legislation in 2006: 801 - the Title VIII--Acquisition Policy, Management, and related matters House Conference Report 109-360 (United States House of Representatives, 2006) that requires the MDA for MDAP/MAIS programs to certify, among other things, that all technologies have been demonstrated in a relevant environment (TRL 6) for all technologies prior to MS B.

2. Non DoD Industry

There is very little written about formal technology readiness assessments by industry. GAO/NSAID report 99-162 (GAO, 1999) interviewed commercial industry and found that in general Industry waits until a technology is equivalent to a TRL 8 before integration into a product. The report contends that:

> …leading commercial firms' practices have produced results that resemble those sought by DOD: more technically advanced, higher quality products, developed in significantly less time, and less expensively than their predecessors…The commercial firms "managing the development of advanced technology differently--and separately--from the development of a product has been key to these results. The firms insist that advanced technology reach a high level of maturity, the point at which the knowledge about that technology is essentially complete, before allowing

> it into a product development. By separating the two, the firms lessen the product manager's burden and place that person in a better position to succeed in delivering the product.

In working with the Venture Capital community during 2003, I found that the Venture Capitalists (VCs) and other technology incubators use an informal assessment process much like the DoD's independent review process by the S&T Executives except the assessment in done in the context of business and market due diligence analogous to DoD's operational environment.

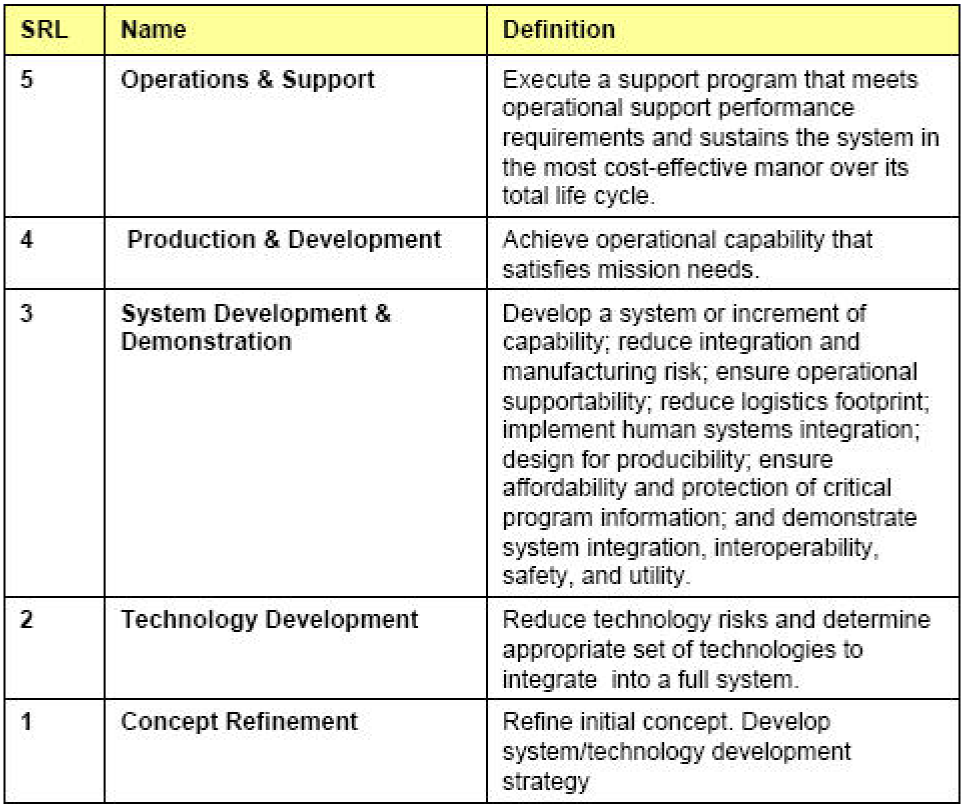
3. Academia

Sauser et al. from the Stevens Institute of Technology has proposed two additional readiness levels in his paper 'From TRL to SRL: The Concept of Systems Readiness Levels (Sauser et al., 2006).' Sauser et al. contends that the use of the NASA/DoD TRLs doesn't take in account the technology within a system, the interactions between the combination of technologies within a system and the interoperability between systems.

Sauser et al. defines System Readiness Levels (SRL) to be defined by the current state of development of a system per DoDs acquisition phases of system development (e.g., SDD). The SRL is a function of the individual Technology Readiness Levels (TRL) in a system and their subsequent integration points with other technologies, called an Integration Readiness Level (IRL). See Figure 23 for a full list of SRL levels and definitions.

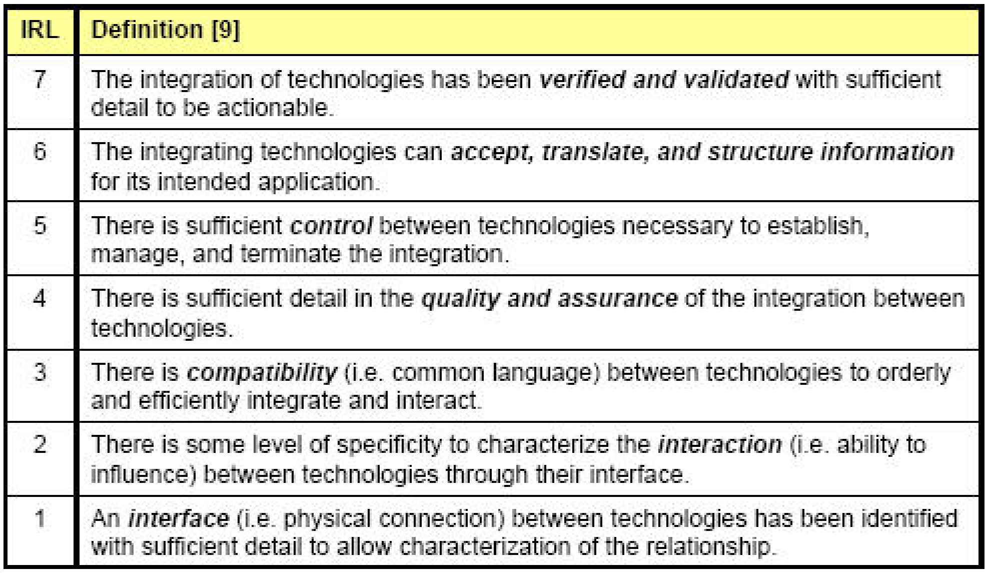
Sauser et al. defines the IRL as systematic measurement of the compatible interactions for various technologies and the consistent comparison of the maturity between integration points. It's a measure of the maturity of combining and coordinating of separate components into a seamless unit. See Figure 24 for a list of IRL levels and definitions.

Sauser et al. has a concept as seen in Figure 25 of how SRL is a function of component TRLs and the IRLs between them. Sauser et al. is continuing to work on these concepts.



SRL	Name	Definition
5	**Operations & Support**	Execute a support program that meets operational support performance requirements and sustains the system in the most cost-effective manor over its total life cycle.
4	**Production & Development**	Achieve operational capability that satisfies mission needs.
3	**System Development & Demonstration**	Develop a system or increment of capability; reduce integration and manufacturing risk; ensure operational supportability; reduce logistics footprint; implement human systems integration; design for producibility; ensure affordability and protection of critical program information; and demonstrate system integration, interoperability, safety, and utility.
2	**Technology Development**	Reduce technology risks and determine appropriate set of technologies to integrate into a full system.
1	**Concept Refinement**	Refine initial concept. Develop system/technology development strategy

Figure 22. System Readiness Levels [From: Sauser et al., 2006]



IRL	Definition [9]
7	The integration of technologies has been ***verified and validated*** with sufficient detail to be actionable.
6	The integrating technologies can ***accept, translate, and structure information*** for its intended application.
5	There is sufficient ***control*** between technologies necessary to establish, manage, and terminate the integration.
4	There is sufficient detail in the ***quality and assurance*** of the integration between technologies.
3	There is ***compatibility*** (i.e. common language) between technologies to orderly and efficiently integrate and interact.
2	There is some level of specificity to characterize the ***interaction*** (i.e. ability to influence) between technologies through their interface.
1	An ***interface*** (i.e. physical connection) between technologies has been identified with sufficient detail to allow characterization of the relationship.

Figure 23. Integration Readiness Levels [From: Sauser et al., 2006]

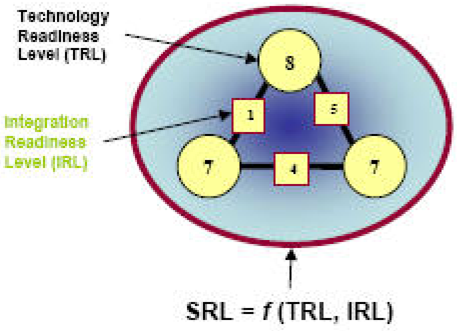

Technology Readiness Level (TRL)
Integration Readiness Level (IRL)
8
1
5
7
4
7
SRL = f (TRL, IRL)

Figure 24. SRL and TRL and IRL [From: Sauser et al., 2006]

THIS PAGE INTENTIONALLY LEFT BLANK

III. RESEARCH

A. RESEARCH APPROACH

Definitions of SoS and FoS and a taxonomy for degrees of interoperability are derived from the literature review. Requirements and guidelines for conducting a SoS TRA will be developed. A short checklist will be developed for identifying where SoS technologies are located to facilitate analyzing the number of systems that are part of the SoS and the potential for unexpected results. The 'system' definitions, interoperability taxonomy, SoS TRA requirements and guidelines and SoS technology locator checklist will be used in the analysis of four possible SoS with respect to the thesis research questions.

Research questions:

1. What are the appropriate definitions of SoS in the context of conducting TRAs? [Section III B.]
2. What are the appropriate definitions for interoperability and its use in defining the operational relevant environment for conducting SoS TRAs? [Section III C.]
3. What is the approach for determining critical technology elements for SoS? [Section III D.]
4. What are the fundamental requirements and guidelines for conducting a SoS TRA and how are these different from a system TRA? [Section III D.]
5. What technology development and acquisition strategies should be employed for technology maturation for SoS given the challenges of synchronization of individual system acquisition schedules? [Identify challenges during FoS/SoS analysis]
6. When is the 'right' time to hold SoS acquisition milestones given the synchronization issues with the individual systems that make up the SoS? [Identify challenges during FoS/SoS analysis]

Research questions 5 and 6, respectively are facilitated by analysis of the technical and systemic challenges. This research will answer whether the SoS/FoS under analysis experienced any of these challenges and how they handled them.

Technical challenges:

a) Capability requirements and functional analysis should occur prior to specific system requirements, system functional analysis, and system technology development; however, many SoS are assembled from legacy systems and network-centric functionality may be constrained

b) Key Performance Parameters (KPPs) or operational requirements for a capability are not easily allocated to individual systems and their subsystems

c) Appropriate SoS relevant environment modeling and simulation and test and evaluation environments will typically be built post system design and development

d) Identification of technology elements given the degree of interoperability or integration may not be obvious within a (re)composable context or environment

e) SoS are typically enabled with software which is easily changed incrementally over time

Systemic challenges:

a) Critical technology developed by the individual programs are in alignment with their respective schedules not the SoS program schedule

b) SoS technology selections and development prior to completion of capability engineering and then individual system(s) engineering drives up risk; SoS engineering needs to be at least through System Functional Review prior to a MS B decision

c) It's challenging to test the critical technologies in an integrated manner if the individual systems have not had the opportunity to all develop their systems enough to have representative systems for SoS testing (e.g., relevant environment for a integrated heterogeneous distributed system)

d) The fielding of a SoS capability is typically time-phased over several years in capability spirals or increments with differing sets of systems and services

B. ‘SYSTEM’ DEFINITIONS

There clearly is no one set of consistent and agreed to terminology for system, FoS and SoS or the types thereof. If one is conducting a TRA it is imperative to have an understood definition in order to characterize the operational environment. A definition provides the basis for identifying the boundary where KPPs/operational requirement will be measured and therefore the boundary that encompasses the CTEs that support achieving the specified KPPs.

The definition of system that would support the definitions of SoS selected from the literature review is the following from Maier and Rechtin.

System:

> …a collection of things or elements which, working together, produce a result not achievable by the things alone.

This definition was selected based on the fact that for both a system and a SoS that this definition seems to cover both cases given that the definition of SoS is:

System of Systems:

> A set or arrangement of interdependent systems that are related or connected to provide a given capability. The loss of any part of the system will significantly degrade the performance or capabilities of the whole (Chairman of the Joint Chief of Staff, 2007).

The literature review revealed that there is a sense that there are different types of SoS. Maier and Rechtin proposed that there are three types of SoS and the differences are driven by managerial control: Virtual, Voluntary, and Directed (definitions repeated here for the ease of the reader).

- Directed: Directed systems are those in which the integrated SoS is built and managed to fulfill specific purposes. It is centrally managed during long term operation to continue to fulfill those purposes, and any new ones the system owners may wish to address. The component systems maintain an ability to operate independently, but their normal operational mode is subordinated to the central managed purpose. For example, an integrated air defense network is usually centrally managed to defend a region against enemy systems, although its component systems may operate independently.
- Collaborative: Collaborative systems are distinct from directed systems in that the central management organization does not have coercive power to run the system. The component systems must, more or less, voluntarily collaborate to fulfill the agreed upon central purposes. The Internet is a collaborative system. The IETF works out standards, but has no power to enforce them. Agreements among the central players on service provision and rejection provide what enforcement mechanism there is to maintain standards. The Internet began as a directed system, controlled by the Advanced Research Projects Agency, to share computer resources. Over time it has evolved from central control through unplanned collaborative mechanisms.

- Virtual: Virtual systems lack a central management authority. Indeed, they lack a centrally agreed upon purpose for the SoS. Large scale behavior emerges, and may be desirable, but the supersystem must rely upon relatively invisible mechanisms to maintain it. A virtual system may be deliberate or accidental. Familiar examples of what is called here a virtual system are the World Wide Web and national economies. Both 'systems' are distributed physically and managerially. The World Wide Web is even more distributed than the Internet in that no agency ever exerted real central control. Control has been exerted only through the publication of standards for resource naming, navigation, and document structure. Web sites choose to obey the standards or not at their own discretion. The system is controlled by the forces that make cooperation and compliance to the core standards. The standards do not evolve in a controlled way; rather they emerge from the market success of various innovators. National economies and the social 'systems' that surround us might be thought of as virtual systems. Politicians regularly try to architect these systems, sometimes through forceful means, but the long-term nature is determined by highly distributed, partially invisible mechanisms.

The TRA Deskbook proposes the following types of IT systems (definitions repeated here for the ease of the reader).

- Business systems – off-the-shelf information system components and COTS software assembled together in a new environment to support the business and management functions of an organization
- Net-reliant (battle management) systems – typically command and control; battle management systems; or intelligence, surveillance, and reconnaissance systems. The net-reliant system is characterized by an intense real-time requirement
- Network infrastructure (or services provider) - backbone and services systems for network management, management of large databases and glue logic to execute and retrieve services across a Wide Area Network of varying security levels.
- Embedded systems - functionality is enabled by IT but not driven by IT itself. Embedded systems emphasize using computer hardware and software to automate internal functions of a weapon system such as platform control and status, sensor signal and data processing, and weapons tasking.

The following SoS types are proposed.

- SoS Service Oriented Architecture (SOA) – this is a combination of Virtual, Business systems, and Net-reliant giving the sense that a system can join the SoS if compliant with it's standards and protocols in order to obtain or supply services.

- SoS Common Operating Environment (COE) – this is a combination of Directed, Net reliant and Network management since in DoD these are typically combined and controlled to provide functionality to a SoS via a network. The level of connectedness is engineered for a specific SoS rather than generic; it may include common applications but not common distributed processing.
- SoS Common Distributed Processing (CDP) – this a combination of Directed and an embedded system approach; embedded doesn't seem to capture the idea of distribution of the processing by all elements of the SoS simultaneously. The level of connectedness is at a common processing (data/algorithm) level vice a common application level. It most likely will include elements of network and network management to accomplish the common distributed processing

The following Family of Systems definition is selected from CJCSI 3170 and the Defense Acquisition Guide (Chapter 4.2.6):

> Family of Systems:
>
> …a set of systems that provide similar capabilities through different approaches to achieve similar or complementary effects (Chairman of the Joint Chief of Staff, 2007)," and "A family of systems does not create capability beyond the additive sum of the individual capabilities of its member systems (USD(AT&L), 2006).

This thesis is primarily focusing on real-time warfighting systems and will follow up on SoS SOA and FoS at a future date.

The definition of SoS gives rise to the idea of systems that are assembled together within a boundary to provide a specified capability. This implies that the systems need to be able to interoperate in a pre-defined manner in order to be able to predict that the 'whole' will deliver the required capability.

C. INTEROPERABILITY TAXONOMY

Interoperability is another word that has no consistent terminology or use as found by the literature review; however, articulating basic types of or intents of communication facilities the ability to discuss the degree or types of interoperability required. Communication is a broadcast and/or two/multiple way exchange of data/information; intent of the communications will drive the types of data/information/knowledge exchanges and the timing of same.

For DoD interoperability, the assumption is made that communications or interoperability is supporting the accomplishment of a task or mission as specified in the DoD definition of interoperability. SEI's definition of interoperability is selected for use in assisting in defining degrees of interoperability:

> The ability of a collection of communicating entities to (a) <u>share</u> specified information and (b) operate on that information according to a <u>shared operational semantics</u> in order to achieve a <u>specified purpose</u> in a given context.

In the literature review it was found that communication consists of the following elements: content (*what type of things are communicated*), source (*by whom*), form (*in which form*), channel (*through which medium*), destination/receiver (*to whom*) and purpose aspect (*with what kind of desired results*). Also, it was found that the purpose of communications with respect to tasks generally falls into the following categories of accomplishing a task or mission: Contribute - to supply, Coordinate – to bring into a common action, movement, or condition, Cooperate - to act or work with another or others**:** act together or in compliance, Collaborate - to work jointly with others or together, Direct - to regulate the activities or course of.

The following expanded definitions and associated attributes for these communication types are proposed to support defining degrees of interoperability for military operations:

a) Contribute – Provide data/information that supports situational awareness. [Independent function] Data/Information is provided when processed by the system and receiving system is available and able to receive the data/information; no timeliness is associated with contributing data/information that is not specifically tied to a mission.

b) Coordination – determining how and when to share resources for differing tasks. Two or more systems execute tasks that are independent from each other and require use of the same resources. These differing tasks could be done without coordination if there were enough resources; however, coordination is required when there are not enough resources to do both tasks simultaneously. [Independent function] Data/information is provided as requested or required and is the minimum required to indicate the need, timelines etc.

c) Cooperation – the action of multiple systems working together on a mission by accomplishing separate and distinct tasks. [Independent (loose coupling) - systems are independent and are allocated differing tasks that are required for a mission and so performance of the mission is dependent on all systems, may have emergent behavior given the interdependencies, bounded system that can be extended.] Data/information is provided in a timely fashion and includes data elements that are shared within the context of the common mission.

d) Collaboration – the action of at least two differing systems working together on one task by accomplishing similar actions to accomplish the task. [Interdependent (tight coupling/synchronized) – Note systems are independent and are collaborating on one task that depends on all systems to accomplish work towards a common task in order to meet performance, bounded system, likely will have emergent behavior given the functional dependencies.] Data/information is provided in real-time to near real-time and includes multiple data elements that are shared within the context of the task and the common mission.

e) Command and Control – Directive – one system tells the other system(s) what to do, when, how, etc. Timelines can be real time (do it now) to non-real time (planning). [Independent – Note systems may be providing for local or remote command and/or control of resources or actions] Data/information is provided in real-time to non-real time and is date elements are small in number.

Degrees of Interoperability based on these definitions are found in Table 5. These basic communication types drive the amount, specific data/information elements, data flows and timeliness of the communications. The amount of data and the temporal aspects of the communication generally are minimal for independent systems, greater for systems that are interdependent, and greatest for systems that are interdependent on one another to provide a capability.

Attribute	**Contribute**	**Coordinate**	**Cooperate**	**Collaborate**	**Command and Control**
Coupling	None	None	Loose	Tight	Varies
Timeliness	None Req	Not Req	Near Real Time	Real Time	Varies
System Type	Independent	Independent	Independent	Interdependent	Independent
Data/Info Type	Information	Information	Data/Info	Data	Information
# of data elements	Small	Small	Small/medium	Large	Small

Table 5. Degrees of Interoperability

The SEI's LISI model proposes the following interoperability taxonomy: Isolated – non-connected with manual inputs, Connected – electronic connection with separate data and applications using homogeneous data exchange mechanisms, Functional – minimal common functions with separate data and applications using heterogeneous data exchange for basic collaboration, Domain – shared data with separate applications using shared databases, and Enterprise – interactive manipulation with shared data and applications using automated distributed information exchange applications.

Alberts et al. Networking the Force Mental Model (seen here again in Figure 26) provides for a functional view of communications. Table 6 compares and contrasts the different interoperability mappings.

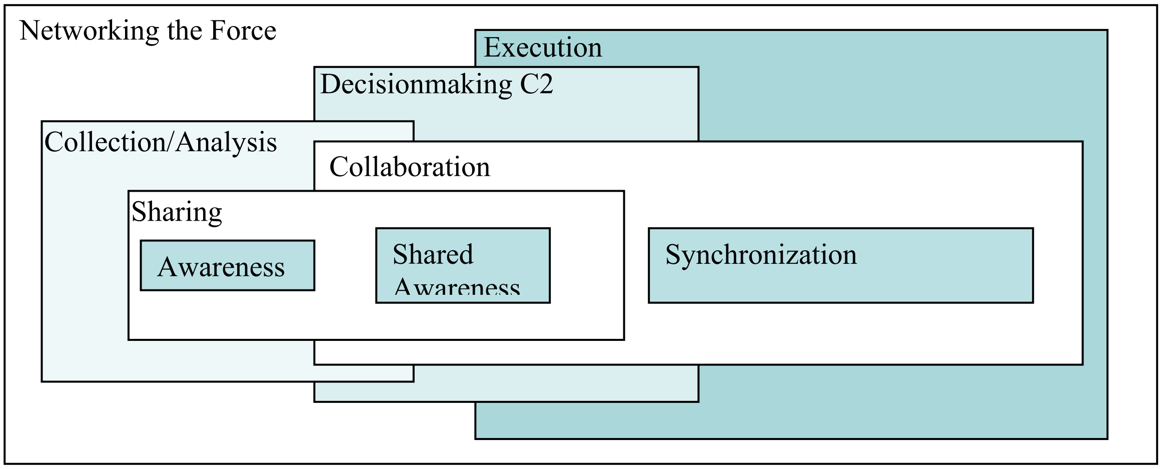


Figure 25. Networking the Force Mental Model [From: Alberts et al., 2001]

COMPARISON OF INTEROPERABILITY MODELS			
Communication Model	**LISI**	**Alberts et al. Mental Model**	**OSI**
Command and Control	-	Decisionmaking/C2 (Shared Awareness)	-
Collaborate	Enterprise	Decisionmaking/C2 (Shared Awareness) Execution (Synchronization)	Application, Presentation, Session
Cooperate	Domain	Sharing (Shared Awareness)	Application, Presentation, Session
Coordinate	Functional	Sharing (Shared Awareness)	Transport, Network, Data Link, Physical
Contribute	Connected	Collect (Awareness)	Transport, Network, Data Link,Physical
-	Not Connected	-	-

Table 6. Comparison of Interoperability Models

For this thesis, the following degrees of interoperability as defined above will be used for the analysis to assist in defining the operational relevant environment and for enabling technology location and identification. Command and Control will be treated in the context in which it is used; for example if it is used for real-time execution of operations, it will be treated as Level 4.

Degrees of Interoperability: Level 0 – Connectionless (self explanatory)

Level 1 - Contribute

Level 2 - Coordinate

Level 3 - Cooperate

Level 4 - Collaborate

D. SYSTEMS OF SYSTEMS TECHNOLOGY READINESS ASSESSMENT REQUIREMENT/GUIDELINES

The TRA Deskbook provides a good set of system TRA requirements and guidelines. There are no specific requirements or guidance regarding SoS in the TRA

Deskbook. Given a SoS is a system that is a set of systems, the current system TRA guidance can be easily extended. The following guidelines are recommended with respective to SoS TRAs in addition to the current system guidelines.

1. Clearly describe the type of SoS and degree of interoperability required – (SOA, COE, or CDP) and provide rationale.
2. Indicate which if any of the systems of the SoS is part of another SoS or FoS (name related programs).
3. Identify SoS spirals/blocks or other expected increments and their timeframes including spirals/blocks of specific systems of the SoS. Provide list of expected changes in architecture, performance, functionality and technology.
4. In the SoS TRA include all CTEs required to meet SoS KPPs/operational requirements; include SoS unique CTEs as well as system unique CTEs required for the specific system to participate as a system of the SoS (e.g., a new radio) regardless of who is responsible for funding or developing.
5. Provide an update to the SoS TRA when any of the systems of the SoS are going thru a spiral upgrade independently of the SoS. Each system of the SoS needs to be assessed for any changed technology or technology implementation to assure SoS performance is preserved.
6. SoS Milestones B and C shall be scheduled post system Milestone Bs and Milestone C's for SoS (or at least in the same timeframe, +/- 3 months). Specific systems need to demonstrate TRL 6 and TRL 7 prior to demonstrating SoS TRL 6 and SoS TRL 7.
7. Systems that are part of a SoS shall include SoS CTEs in their system (SoS in the case of a IAMD SoS) specific TRA. Each individual system will need to develop their system specific technologies to a TRL 6 and above as well as demonstrate system functionality with SoS specific technologies to a TRL 6 and above.
8. All SoS CTEs whether part of the SoS or part of the specific systems of the SoS, shall be assessed against SoS requirements. These assessments should begin as early as possible and should begin at TRL 3 assessments.

If a Program Review is used to initiate the SoS, direction shall be provided to systems of the SoS to begin SoS Engineering activities including technology development and assessment. All SoS CTEs including the system specific CTEs for SoS activities need to be matured prior to SoS MS B. The synchronization and technology maturation strategy shall be identified in the Acquisition Decision Memorandum and defined in the Acquisition Strategy and TDS.

E. SOS TECHNOLOGY LOCATOR CHECKLIST

It is useful to have a checklist when performing a TRA for a SoS given the number and complexity of systems that generally make up a SoS. Also, it is a challenge to identify where unexpected effects may occur and a checklist will assist in lowering the risk of finding these unexpected effects post SoS development. Generally there is a SoS PM and PMs for each of the systems that make up a SoS. It is recommended that the system program managers and SoS PM coordinate regarding common SoS technologies needs as well as system specific technologies that are required to interface with the SoS technologies. System technologies may not pass the criteria for being a system CTE; however, once a decision is made for the system to be part of the SoS, the CTE in question may become a SoS CTE. Some system specific CTEs may not be a SoS CTEs; an example is advanced armor for a tank that is part of FCS would not be part of the FCS SOSCOE CTEs. The technology list should make a distinction between technologies that are common to all systems of the SoS and those technologies that are unique to a specific system of the SoS that is required in order to work in the SoS operational context. If a technology is required to enable a system to meet SoS KPPs/operational requirements it should be included in the SoS CTE list.

A SoS (IT) technology locator/identification checklist is recommended. SoS technology identification requires knowledge of the systems in the SoS, the types of functions and computational processes being performed cooperatively and collaboratively (horizontally and vertically) and the specific functionality and required behavior and performance. Documentation should indicate by what methods these requirements will be achieved: 1) procedures - doctrine, mission, architectures, and standards, 2) applications and 3) hardware/software or a combination thereof. Specific technologies/category of technology should be noted if known. The following interoperability/synchronization related attributes should be used as lines of inquiry when executing the analysis with respect to each facets of the environment - physical, logical, data, security and user.

Interoperability Attribute List:

- Completeness - all relevant items available, including entities, their attributes, and relationships between them

- Correctness - all items in the system faithful representations of the realities they describe
- Currency – latency of the items of information
- Accuracy or Level of Precision - dependent on the purpose
- Consistency - across different systems, applications, functions and data/information/knowledge. Note Data models that the SoS is expected to be in compliance with.
- Connectivity – specified integration of nodes, type of connections, syntactic compatibility, quality of service and bandwidth/data rate requirements
- Capacity – databases, scalability, number and type of applications, processor requirements
- COTS – use of and consideration of obsolescence, instability in standards or availability, security, and reliability

The technology locator/identification checklist should be used to identify all technologies (not just CTEs) in both the SoS and the systems that are part of the SoS (if the particular artifact is not available to the program, a similar design or requirements document should be identified and used). Also, this should be accomplished for each spiral or block of each system and the SoS. If new technologies are identified to meet the requirement and they are not achievable in the timeframe due to unavailability of technologist or there is not enough funding to mature them, this should be noted and a recommended adjustment in requirements and technology solutions propose to the PM. After all technologies have been identified and appropriate technology alternatives the criteria for CTEs can be applied:

1) An approved ICD or draft/approved Capability Description Document whichever is latest: this provides the KPPs/operational requirements.
    a. Evaluate and document how much of an increase or change in capability is being required from currently fielded systems.
    b. Determine and document what current technologies can be modified to meet the new requirements or if the change in capability requires fundamentally new technologies, describe what technologies would be required if known.
2) An OV-1; this provides the operational context and concept.
    a. Document the systems that are in the SoS and what requirements they are now meeting wrt the KPPs and with what technologies

b. Document which systems have worked together in a SoS before or currently and to what ends and what technologies were in common (that are applicable to this specific SoS).

3) An approved/draft concept of employment.

a. Document any major difference between current operations and expected approved/new operations.

b. Document the type of technologies that would be required to enable the new concepts.

4) An approved/draft OV-2 and an approved/draft SV-1 and SV-2; this identifies the specific operational nodes/systems, the operational activities at each node, and the information exchanges and interconnections needed between nodes.

a. Document the connectivity requirements required to enable these activities from the interoperability attribute list above (e.g., bandwidth, types of networks/datalinks) and identify technology requirements.

b. Document the data/information/knowledge exchanges required and identify technology requirements.

5) An approved/draft OV-3 and SV-3; identifies the interfaces and the information exchanges between nodes. Document any new/unusual (special) interfaces or information exchanges that would require new algorithms, methods or techniques to process and/or encode/decode data/information. (document proposed technologies).

6) An approved/draft OV-5; identifies capabilities, relationships among activities and inputs and outputs

a. Document new/modified required capabilities and any new/modified relationships and the technologies needed to enable these.

b. Document new/modified input/outputs and the technologies required that would enable networking, network management, or new processing techniques to meet these capabilities.

7) An approved/draft OV-6; describes the sequencing and timing of activities as well as business rules and processes. An executable simulation is highly desired.

a. Document timing requirements and note those that are more stressing than that currently fielded; propose technologies that would be required to meet these.

b. Document new types of business rules and processes that require new/modified algorithms, techniques and methods – note where there is an expectation of common processing of data across an interface; identify the technologies required.

8) An approved/draft OV-7; documents the data requirements and business rules. Document any special data requirements, business rules and the algorithms, techniques and methods required.

9) An approved/draft SV-4 and SV-5; The SV-4 documents the system functions and the data flow between them and the operational activities supported

   a. Document all major system functions, the operational activities associated with them, the data flows between them and the technologies required to enable these functions. Note those functions that are required for synchronization.

   b. Document all expected interacting technologies and/or have dependencies on other technologies.

10) An approved/draft SV-6 and SV-11 documents the data element exchanges and the physical implementation e.g., messages. Document any technology requirements to enable the data flow and implementation in a physical architecture.

11) An approved/draft SV-7; documents the performance characteristics including the timelines. Document technologies and their requirements to meet functional, behavioral and performance requirements

12) An approved/draft TV-1 and TV-2 – current and future standards; document which standards are required for the systems and identify new/modified technologies that are required.

13) Review proposed list of new/modified technologies/subsystem/systems to determine if technology may impact the following or may be limited in its use; identify possible technology options that will not adversely impact operational resources:

   a. Manning impacts: In-theater, reach-back capabilities, Knowledge /Skills/Ability requirements changes for current billets.

   b. New data requirements, new security/information assurance requirements and technologies required to meet these requirements.

   c. New/Modifications in operational procedures (Service, Joint, Coalition).

   d. New/Modifications in logistic or other support requirements (e.g calibration resources, batteries).

   e. New/Modification in operational planning.

   f. New/Modifications in IT support/databases/network equipment etc.

   g. New/Modifications in training.

   h. Adversely impact operational budgets.

i. Require legal or other policy changes including impacts on the environment (overseas laws and standards may differ from those of the United States).

j. Impact health and/or safety.

Figure 27 provides a good summary of the analysis that this checklist embodies. Ideally this analysis is performed collaboratively between the S&T and acquisition teams supporting the SoS Engineering activities. At the end of the analysis one should have a complete list of new/modified/current technologies and/or category of technologies being used, planned for use, or require development in order to achieve the SoS KPPs mapped to the operational architecture, system architecture and physical architectures.

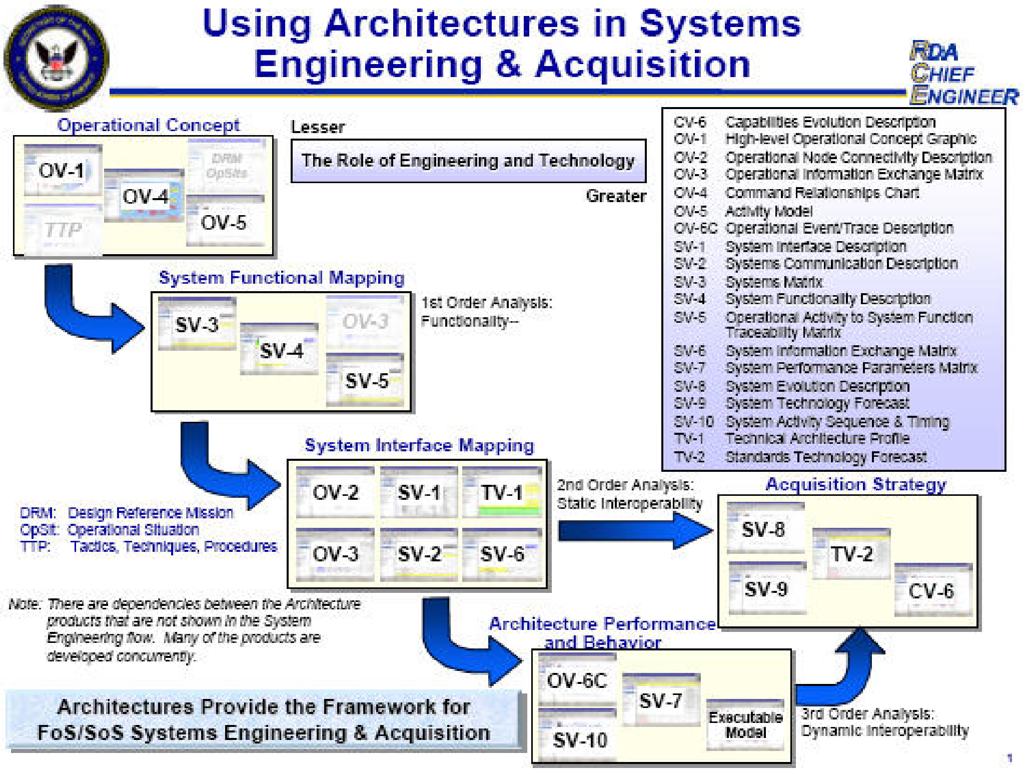
This list can then be vetted against the CTE criteria found in the TRA Deskbook to determine the CTEs that should be addressed in a TRA.

F. SELECTED DOD PROGRAM ANALYSIS

Four DoD programs are analyzed with respect to the research questions.

1. Theater Battle Management Command System

From the literature review, TBMCS is a set of applications used to collect, process and distribute data in support of the AOC. The AOC has been described as a SoS or a complex system created from an opportunistic aggregation of systems (80+ applications and systems) and has a sense of unboundedness. (See Figure 28 for the set of AOC applications) No ‘two’ AOCs are the same with any probability. Initially it was intended to integrate the functions of three systems major systems: CTAPS, which was under development, the Wing Command and Control System, and the Combat Intelligence System. At the start of the program TBMCS did not have an Operational Requirements Document/CDD or a Concept of Operations on how it was to be used in the field. The system architecture was defined at a high level. These factors made it impossible to test with any established criteria. Testing that did occur did not exercise concurrent processing and the first tests failed (Collens Jr., 2005).



Using Architectures in Systems Engineering & Acquisition

RDA CHIEF ENGINEER

Operational Concept
OV-1
OV-4
DRM OpSits
TTP
OV-5
Lesser
The Role of Engineering and Technology
Greater
System Functional Mapping
SV-3
SV-4
OV-3
SV-5
1st Order Analysis: Functionality--
System Interface Mapping
OV-2
SV-1
TV-1
OV-3
SV-2
SV-6
2nd Order Analysis: Static Interoperability
Acquisition Strategy
SV-8
TV-2
SV-9
CV-6
Architecture Performance and Behavior
OV-6C
SV-7
SV-10
Executable Model
3rd Order Analysis: Dynamic Interoperability
1

CV-6	Capabilities Evolution Description
OV-1	High-level Operational Concept Graphic
OV-2	Operational Node Connectivity Description
OV-3	Operational Information Exchange Matrix
OV-4	Command Relationships Chart
OV-5	Activity Model
OV-6C	Operational Event/Trace Description
SV-1	System Interface Description
SV-2	Systems Communication Description
SV-3	Systems Matrix
SV-4	System Functionality Description
SV-5	Operational Activity to System Function Traceability Matrix
SV-6	System Information Exchange Matrix
SV-7	System Performance Parameters Matrix
SV-8	System Evolution Description
SV-9	System Technology Forecast
SV-10	System Activity Sequence & Timing
TV-1	Technical Architecture Profile
TV-2	Standards Technology Forecast

DRM:	Design Reference Mission
OpSit:	Operational Situation
TTP:	Tactics, Techniques, Procedures

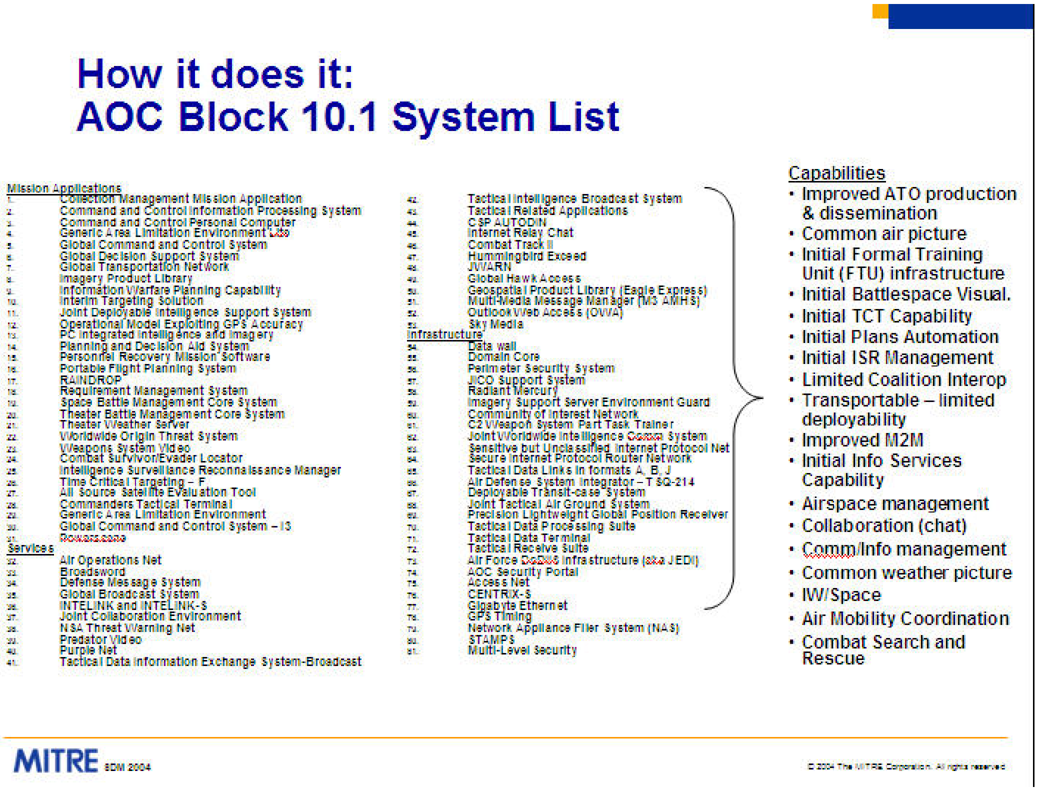
Note: There are dependencies between the Architecture products that are not shown in the System Engineering flow. Many of the products are developed concurrently.

Architectures Provide the Framework for FoS/SoS Systems Engineering & Acquisition

Figure 26. Using Architecture in System Engineering [From: Dickerson and Soules, 2002]

Eventually the TBMCS program established high level requirements and put in place a process to establish system requirements and engineering processes. TBMCS was directed to use DII COE. TBMCS has evolved from a large client-server application to a much more streamlined, web-based enterprise over the last few years. These actions provide a way for the program to progress more successfully.

The following figures show the operational and system architectures for TBMCS. Figure 29 - TBMCS Notional Theater C4I, Figure 30 - TBMCS Functional Description, Figure 31 - TBMCS interfaces, Figure 32 - TBMCS with DII COE, Figure 33 - TBMCS Communication Architecture and Figure 34 TBMCS Data Architecture.



How it does it:
AOC Block 10.1 System List

Mission Applications

1. Collection Management Mission Application
2. Command and Control Information Processing System
3. Command and Control Personal Computer
4. Generic Area Limitation Environment Lite
5. Global Command and Control System
6. Global Decision Support System
7. Global Transportation Network
8. Imagery Product Library
9. Information Warfare Planning Capability
10. Interim Targeting Solution
11. Joint Deployable Intelligence Support System
12. Operational Model Exploiting GPS Accuracy
13. PC Integrated Intelligence and Imagery
14. Planning and Decision Aid System
15. Personnel Recovery Mission Software
16. Portable Flight Planning System
17. RAINDROP
18. Requirement Management System
19. Space Battle Management Core System
20. Theater Battle Management Core System
21. Theater Weather Server
22. Worldwide Origin Threat System
23. Weapons System Video
24. Combat Survivor/Evader Locator
25. Intelligence Surveillance Reconnaissance Manager
26. Time Critical Targeting – F
27. All Source Satellite Evaluation Tool
28. Commanders Tactical Terminal
29. Generic Area Limitation Environment
30. Global Command and Control System – I3
31. Powerscene

Services

32. Air Operations Net
33. Broadsword
34. Defense Message System
35. Global Broadcast System
36. INTELINK and INTELINK-S
37. Joint Collaboration Environment
38. NSA Threat Warning Net
39. Predator Video
40. Purple Net
41. Tactical Data Information Exchange System-Broadcast
42. Tactical Intelligence Broadcast System
43. Tactical Related Applications
44. CSP AUTODIN
45. Internet Relay Chat
46. Combat Track II
47. Hummingbird Exceed
48. JWARN
49. Global Hawk Access
50. Geospatial Product Library (Eagle Express)
51. Multi-Media Message Manager (M3 AMHS)
52. Outlook Web Access (OWA)
53. Sky Media

Infrastructure

54. Data wall
55. Domain Core
56. Perimeter Security System
57. JICO Support System
58. Radiant Mercury
59. Imagery Support Server Environment Guard
60. Community of Interest Network
61. C2 Weapon System Part Task Trainer
62. Joint Worldwide Intelligence Comm System
63. Sensitive but Unclassified Internet Protocol Net
64. Secure Internet Protocol Router Network
65. Tactical Data Links in formats A, B, J
66. Air Defense System Integrator – TSQ-214
67. Deployable Transit-case System
68. Joint Tactical Air Ground System
69. Precision Lightweight Global Position Receiver
70. Tactical Data Processing Suite
71. Tactical Data Terminal
72. Tactical Receive Suite
73. Air Force DoDIIS Infrastructure (aka JEDI)
74. AOC Security Portal
75. Access Net
76. CENTRIX-S
77. Gigabyte Ethernet
78. GPS Timing
79. Network Appliance Filer System (NAS)
80. STAMPS
81. Multi-Level Security

Capabilities

- Improved ATO production & dissemination
- Common air picture
- Initial Formal Training Unit (FTU) infrastructure
- Initial Battlespace Visual.
- Initial TCT Capability
- Initial Plans Automation
- Initial ISR Management
- Limited Coalition Interop
- Transportable – limited deployability
- Improved M2M
- Initial Info Services Capability
- Airspace management
- Collaboration (chat)
- Comm/Info management
- Common weather picture
- IW/Space
- Air Mobility Coordination
- Combat Search and Rescue

MITRE SDM 2004

© 2004 The MITRE Corporation. All rights reserved

Figure 27. AOC System List [From: Norman and Kuras, 2004]

a. TBMCS SoS or Not?

TBMCS is assessed to be a collection of systems facilitated by a COE (DII COE), but are not interdependent (not a SoS) on each other to accomplish their specific tasks and not a FoS that would have differing systems to accomplish the same mission. It may be useful to call it an Enterprise (a systematic purposeful activity (Merriam-Webster, 2007).

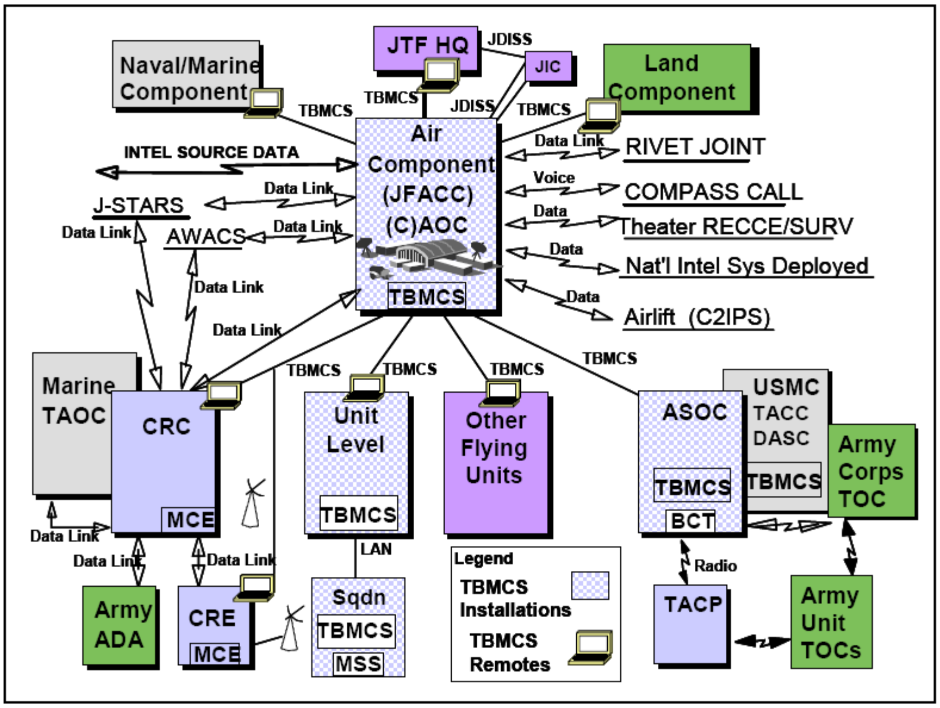


Figure 28. Notional Theater C4I [From: Collens Jr. and Krause, 2005]

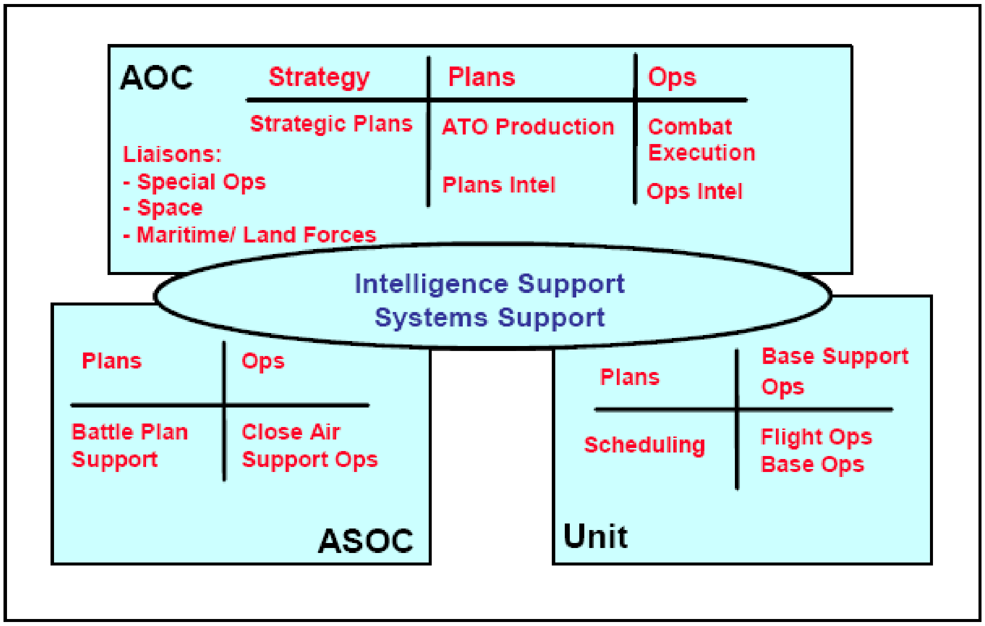


Figure 29. TBMCS Functional Description [From: Collens Jr. and Krause, 2005]

b. TBMCS Interoperability

It operates with other systems via contribution (Level 1), coordination (Level 2) and cooperation (Level 3) and appears to operate as an Enterprise. It is not evident TBMCS is driven by real-time collaboration of simultaneous work on the same task; Cooperation regarding a mission is facilitated by the COE but not necessarily enabled by it. The TBMCS has its own database and added functionality to the DII COE for various applications.

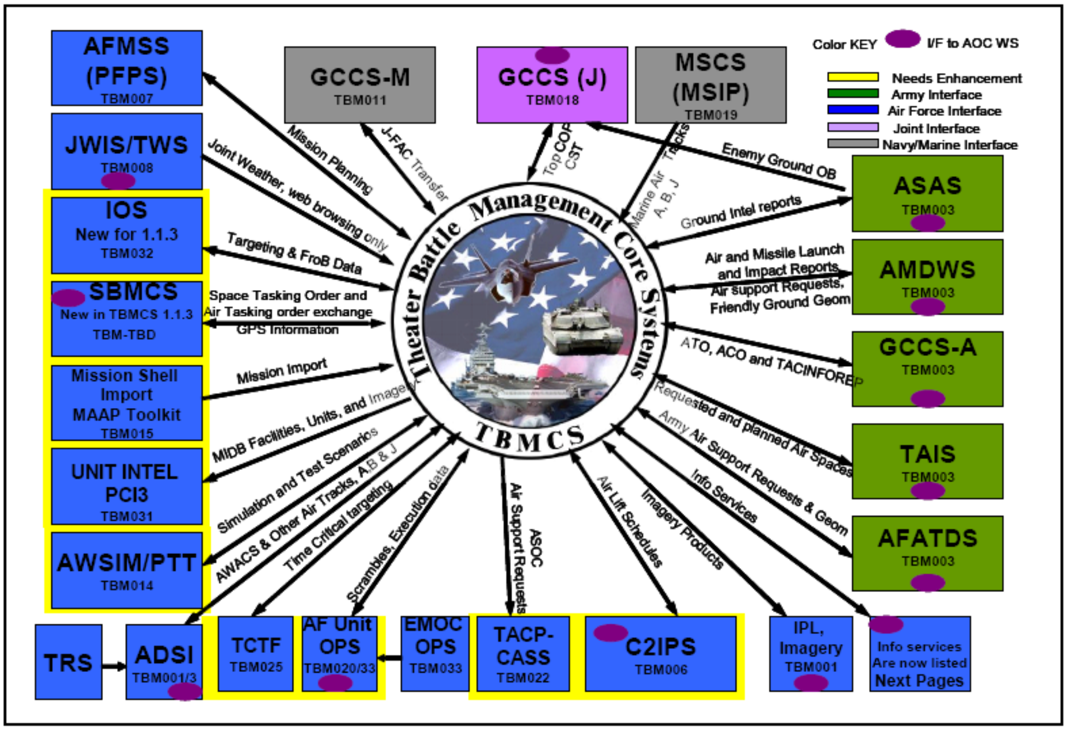


Figure 30. TBMCS Interfaces V1.1.3 [From: Collens Jr. and Krause, 2005]

The most important interoperability attributes for TBMCS are:

- Completeness - all relevant items available, including entities, their attributes, and relationships between them
- Correctness - all items in the system faithful representations of the realities they describe
- Accuracy or Level of Precision - dependent on the purpose
- Connectivity – specified integration of nodes, type of connections, syntactic compatibility, quality of service and bandwidth/data rate requirements

- Capacity – databases, scalability, number and type of applications, processor requirements
- COTS – use of and consideration of obsolescence, instability in standards or availability, security, and reliability

The other attributes while important, were not drivers for CTEs.

c. TBMCS TRA Requirements and Guidelines

TBMCS has defined spirals with the emphasis on all systems using the DII COE. Systems are expected and encouraged to bring themselves into the TBMCS ‘enterprise’. It’s unclear what coordination or engineering occurs between the TBMCS and system PMs.

There was no formal declaration of TBMCS as a SoS or FoS program. Synchronization of specific applications or programs is not evident from a planning perspective. It’s unclear that a TRA for TBMCS was considered; applications or systems are required to mature their own systems. It is unknown whether system TRAs included the DII COE elements in their TRA.

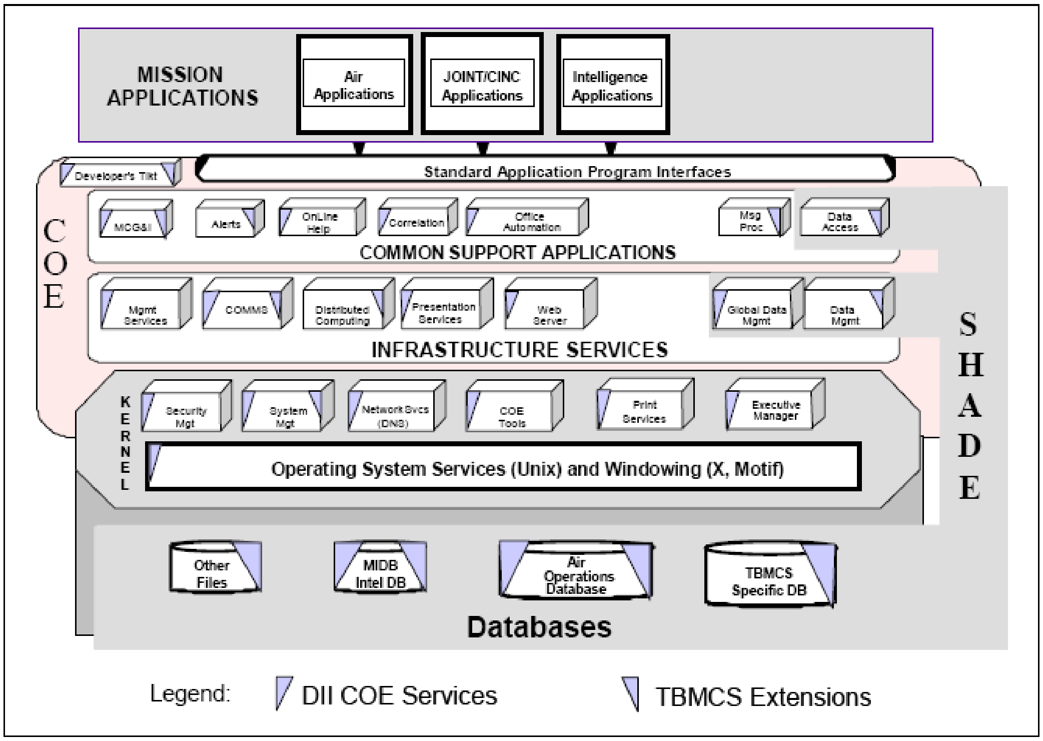


Figure 31. TBMCS with DII COE II Architecture [From: Collens Jr. and Krause, 2005]

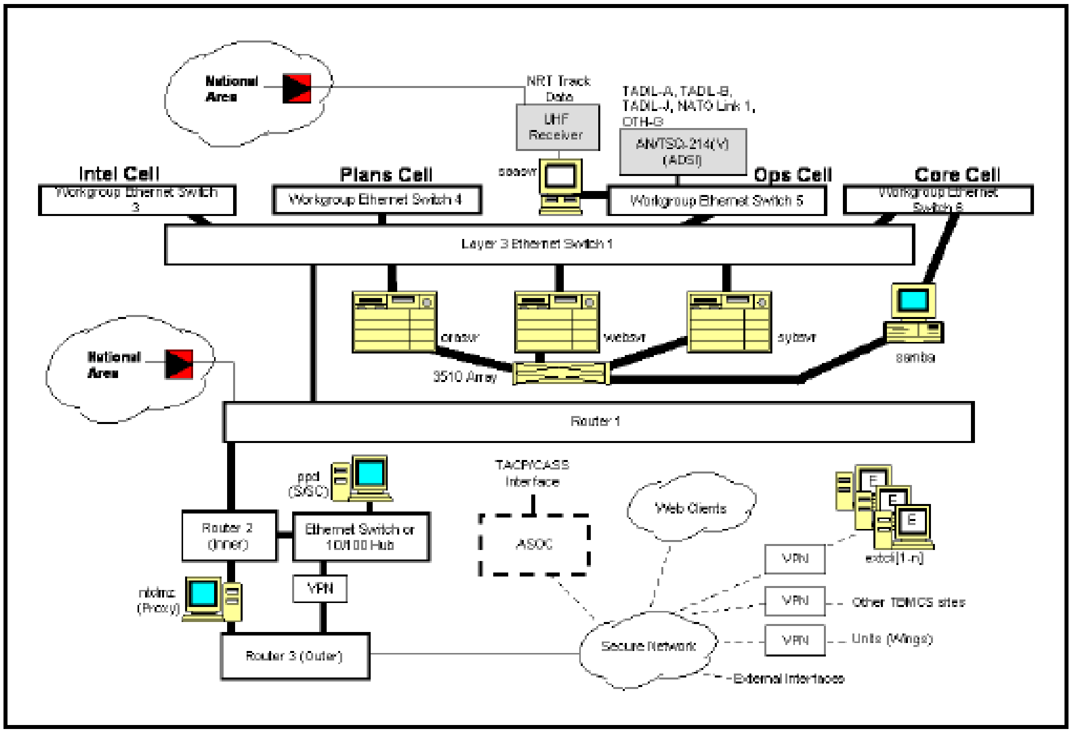


Figure 32. TBMCS Communications Architecture [From: Collens Jr. and Krause, 2005]

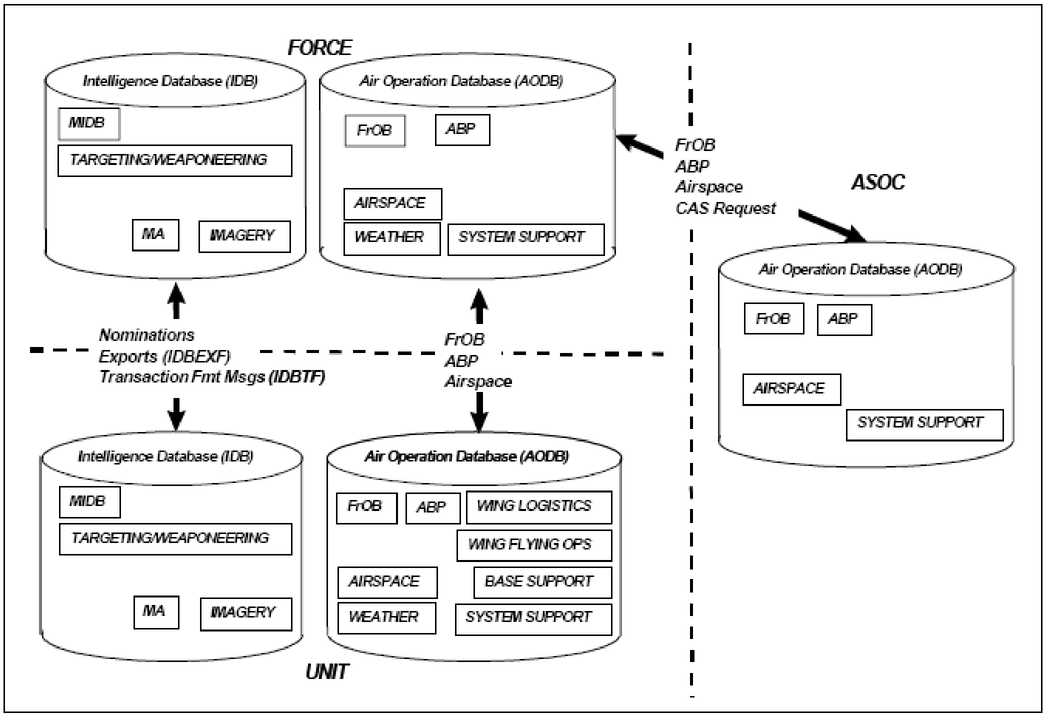


Figure 33. TBMCS Data Architecture [From: Collens Jr. and Krause, 2005]

d. TBMCS CTE Identification

TBMCS did not have the usual requirements, architecture and system engineering artifacts. Its unclear whether there were any CTEs identified. Several standards were directed – DII COE and it inherited the differing standards from the legacy systems. TBMCS in it's first rendition was understood by inspection TBMCS was found to have four types of integration which appear to support the degrees of interoperability identified above: 1) internal interfaces and subcomponents, 2) varying level of maturing third party applications, 3) external interfaces, and 4) databases. Fully 90 percent of TBMCS consisted of third-party products or government-furnished equipment (GFE), and a majority of the software was third-party: GOTS or COTS. TBMCS incorporated 76 applications, 64 point-to-point external system interfaces, and 413 segments involving over 5 million lines of software, as well as two commercial relational databases (Collens Jr., 2005). The system had two hardware baselines, and the communications infrastructure the DII COE. The most extensive integration involved data interoperability, and the two primary TBMCS databases – the Air Operations Data Base and the Intelligence Server Data System – followed different standards and were updated at different intervals. The government also mandated the use of specific hardware, which varied depending on the service branch that would use TBMCS. A particular application requested by the user might not integrate well into the system because it did not use the DII COE properly or because its COTS infrastructure was more current than that of TBMCS.

TBMCS applications are now migrating from a client-server system to web-based architecture over various spirals. A TBMCS Developer's Network (DEVNET), a collaborative effort of the Electronic Systems Center (ESC) and Lockheed Martin, enables third-party Air Operations Center (AOC) system developers to easily integrate new applications into TBMCS in a non-proprietary, 'plug and play' open architecture environment.

e. TBMCS Technical Challenges

TBMCS seems to have experienced all the technical challenges a program could possibly encounter. There were no system engineering efforts initially. After high level requirements were established, capability requirements and functional analysis occurred at the same time as system requirements, system functional analysis, and system technology development were being accomplished; however, TBMCS was being assembled from legacy systems. Only over time has TBMCS been able to start to overcome these historical hurdles and move towards network-centric functionality.

It’s unclear that today TBMCS high level performance parameters are allocated to individual systems and their subsystems. TBMCS is changing constantly over time and is enabled with varying different hardware.

f. TBMCS Systemic Challenges

Critical technologies developed by the individual programs don’t appear to be in any particular alignment with an overall TBMCS schedule. No overarching technology development strategy seems evident. It’s unclear what milestones TBMCS and all its systems need to pass through. Testing is challenging, there appear to be selected opportunities for integrated testing.

The fielding of TBMCS capability is time-phased over several spiral upgrades several years apart with a focus on becoming totally web-enabled with systems being able to be incorporated via the DII COE. Program synchronization seems unachievable based on the all-encompassing nature of the program; however, over-time stability of individual applications or systems should increase. This makes sense in the context of an Enterprise.

2. Future Combat System (FCS)

The Army's Future Combat Systems (FCS) currently includes 14 elements plus the network and the soldier (See Figure 35). The network allows the FCS Family-of-Systems (FoS) to operate as a cohesive SoS where the whole of its capabilities is greater than the sum of its parts. The FCS program anticipates needing to interoperate or integrate with as many as 170 systems, some of which are in development and many are legacy. Many complementary programs are not being developed exclusively for FCS and are outside the direct control of the FCS program, such as their communications networks.

The FCS network consists of four overarching building blocks: System-of-Systems Common Operating Environment (SOSCOE); Battle Command (BC) software; communications and computers (CC); and intelligence, reconnaissance and surveillance (ISR) systems. SOSCOE is central to the FCS network, which supports multiple mission-critical applications independently and simultaneously. It is configurable so that any specific instantiation can incorporate only the components that are needed for that instantiation. SOSCOE architecture uses COTS hardware and a DISR compliant operating environment to produce an non-proprietary, standards-based component architecture for real-time, near-real-time, and non-real time applications (Figure 36) (Future Combat System Program Office, 2007). The following figures show the FCS operational, system, and physical architectures: Figure 37 – FCS OV-1, Figure 38 - FCS Communications Architecture, Figure 39 – Network Concept of Operations, Figure 40 - FCS System Architecture, Figure 41 - SoS Approach, and Figure 42 – LANDWARNET.

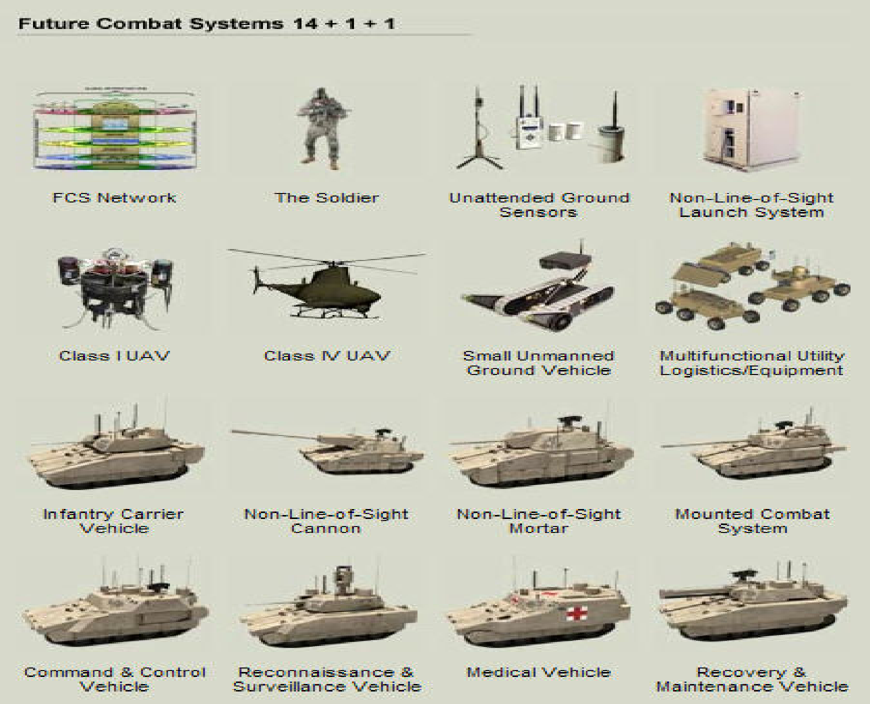

Future Combat Systems 14 + 1 + 1
FCS Network
The Soldier
Unattended Ground Sensors
Non-Line-of-Sight Launch System
Class I UAV
Class IV UAV
Small Unmanned Ground Vehicle
Multifunctional Utility Logistics/Equipment
Infantry Carrier Vehicle
Non-Line-of-Sight Cannon
Non-Line-of-Sight Mortar
Mounted Combat System
Command & Control Vehicle
Reconnaissance & Surveillance Vehicle
Medical Vehicle
Recovery & Maintenance Vehicle

Figure 34. Current FCS 14 +1 +1 [From: Future Combat System Program Office, 2007]

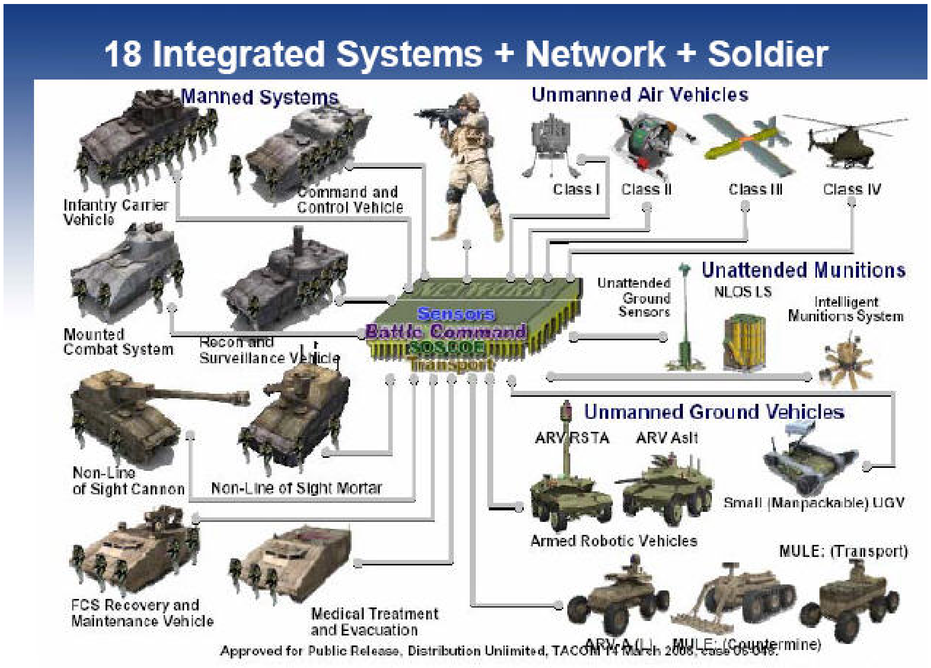


Figure 35. FCS Enabled by SOSCOE [From: Child, 2006]

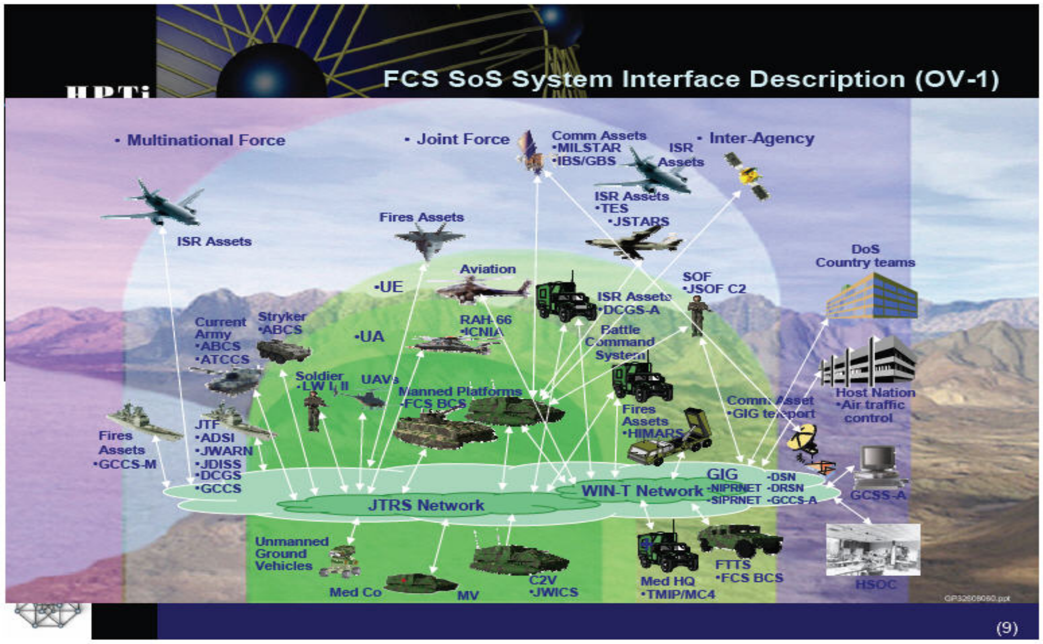
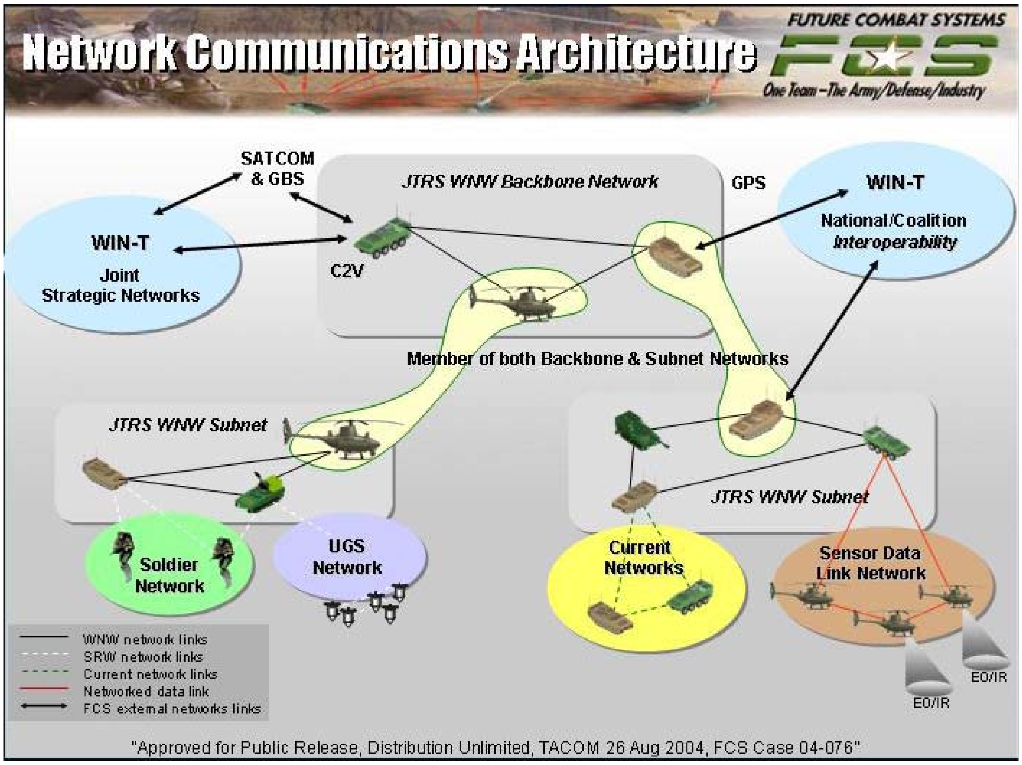


Figure 36. Future Combat System OV-1 [From: Powell, 2006]

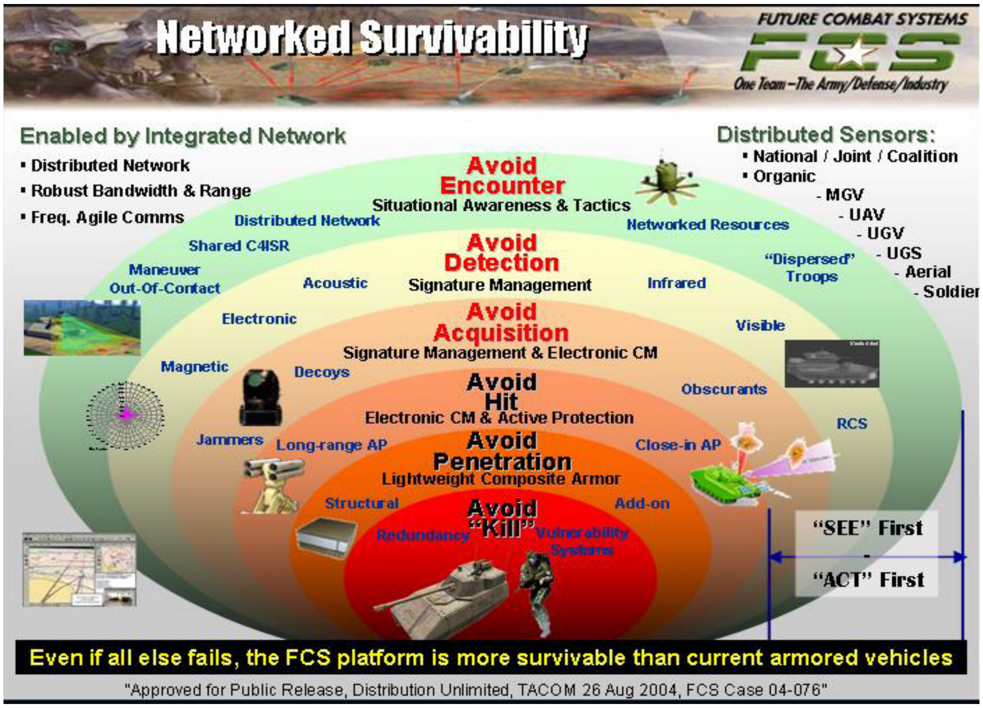


Network Communications Architecture

FUTURE COMBAT SYSTEMS FCS One Team – The Army/Defense/Industry

"Approved for Public Release, Distribution Unlimited, TACOM 26 Aug 2004, FCS Case 04-076"

Figure 37. FCS Communications Architecture [From: Future Combat System Program Office, 2005]



Networked Survivability

FUTURE COMBAT SYSTEMS FCS One Team – The Army/Defense/Industry

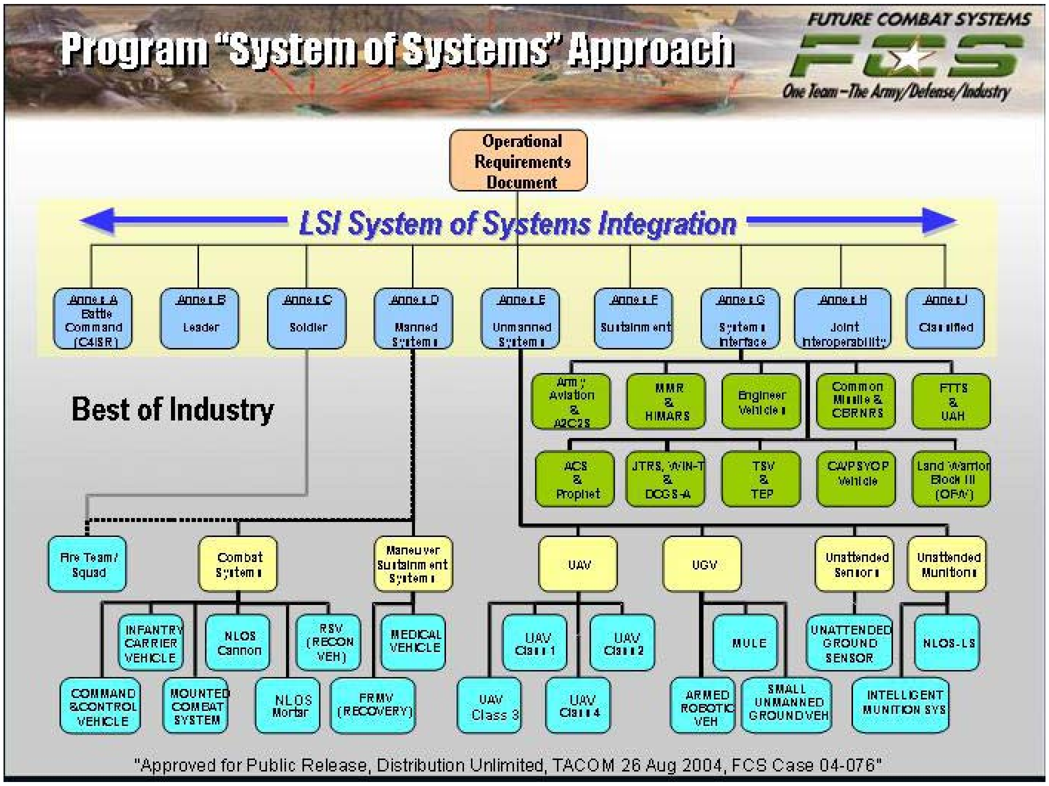
Enabled by Integrated Network
- Distributed Network
- Robust Bandwidth & Range
- Freq. Agile Comms

Distributed Sensors:
- National / Joint / Coalition
- Organic
  - MGV
  - UAV
  - UGV
  - UGS
  - Aerial
  - Soldier

Even if all else fails, the FCS platform is more survivable than current armored vehicles

"Approved for Public Release, Distribution Unlimited, TACOM 26 Aug 2004, FCS Case 04-076"

Figure 38. FCS Network Concept of Operations [From: Future Combat System Program Office, 2005]



Program "System of Systems" Approach

FUTURE COMBAT SYSTEMS

FCS

One Team – The Army/Defense/Industry

Operational Requirements Document

LSI System of Systems Integration

Annex A Battle Command (C4ISR)

Annex B Leader

Annex C Soldier

Annex D Manned Systems

Annex E Unmanned Systems

Annex F Sustainment

Annex G Systems Interface

Annex H Joint Interoperability

Annex I Classified

Best of Industry

Army Aviation & A2C2S

MMR & HIMARS

Engineer Vehicles

Common Missile & CBRNRS

FTTS & UAH

ACS & Prophet

JTRS, WIN-T & DCGS-A

TSV & TEP

CA/PSYOP Vehicle

Land Warrior Block III (OFW)

Fire Team/ Squad

Combat Systems

Maneuver Sustainment Systems

UAV

UGV

Unattended Sensors

Unattended Munitions

INFANTRY CARRIER VEHICLE

NLOS Cannon

RSV (RECON VEH)

MEDICAL VEHICLE

UAV Class 1

UAV Class 2

MULE

UNATTENDED GROUND SENSOR

NLOS-LS

COMMAND &CONTROL VEHICLE

MOUNTED COMBAT SYSTEM

NLOS Mortar

FRMV (RECOVERY)

UAV Class 3

UAV Class 4

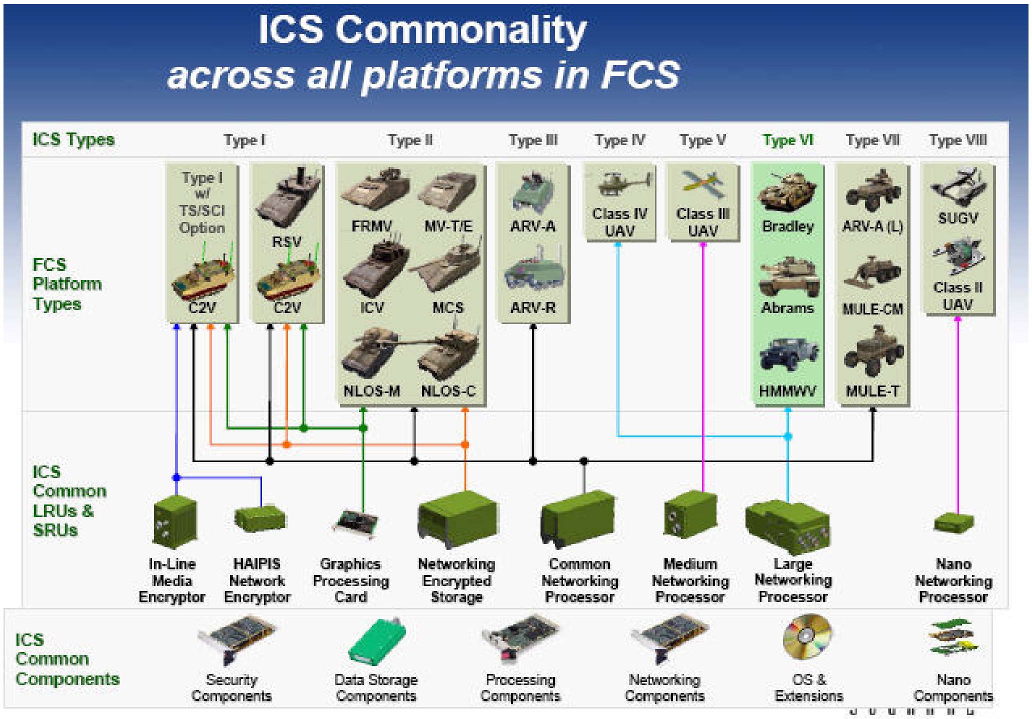
ARMED ROBOTIC VEH

SMALL UNMANNED GROUND VEH

INTELLIGENT MUNITION SYS

"Approved for Public Release, Distribution Unlimited, TACOM 26 Aug 2004, FCS Case 04-076"

Figure 39. FCS System Architecture [From: 36 Future Combat System Program Office 2005]



ICS Commonality
across all platforms in FCS

ICS Types: Type I, Type II, Type III, Type IV, Type V, Type VI, Type VII, Type VIII

FCS Platform Types

Type I w/ TS/SCI Option

C2V

RSV

C2V

FRMV

MV-T/E

ICV

MCS

NLOS-M

NLOS-C

ARV-A

ARV-R

Class IV UAV

Class III UAV

Bradley

Abrams

HMMWV

ARV-A (L)

MULE-CM

MULE-T

SUGV

Class II UAV

ICS Common LRUs & SRUs

In-Line Media Encryptor

HAIPIS Network Encryptor

Graphics Processing Card

Networking Encrypted Storage

Common Networking Processor

Medium Networking Processor

Large Networking Processor

Nano Networking Processor

ICS Common Components

Security Components

Data Storage Components

Processing Components

Networking Components

OS & Extensions

Nano Components

Figure 40. FCS SoS Approach [From: Child, 2006]

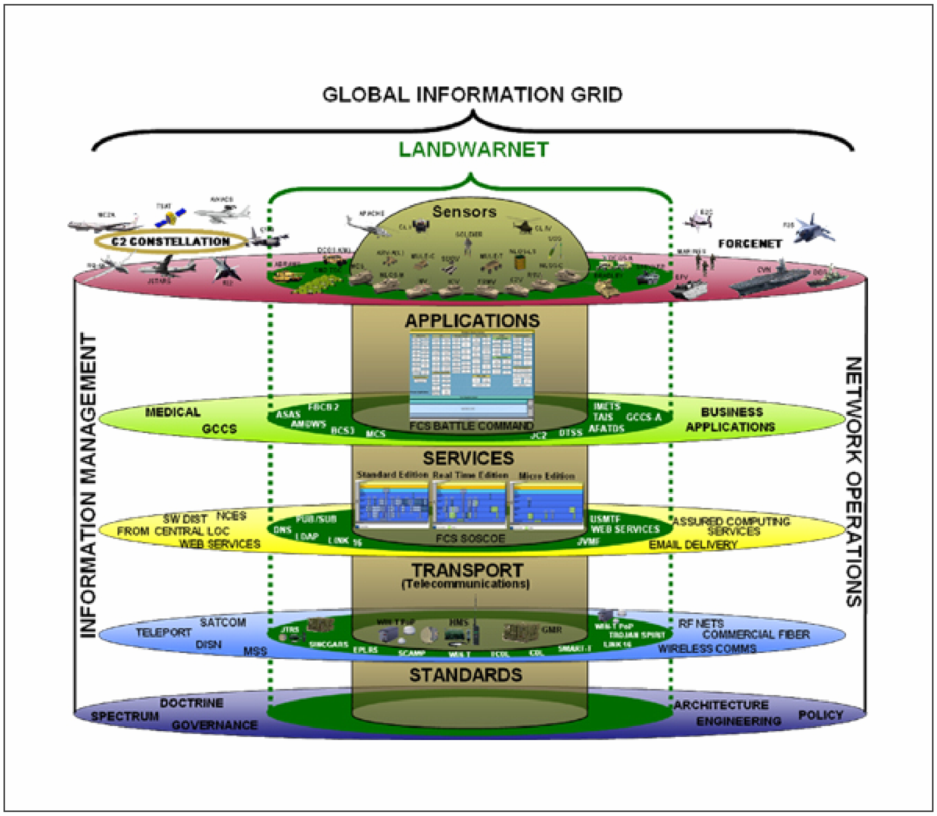


Figure 41. FCS LANDWARNET [From: Future Combat System Program Office, 2007]

a. FCS SoS or Not?

FCS is assessed to be a FoS enabled by FCS SOSCOE. The FCS program is not required to meet performance beyond the capabilities of the individual systems and there seems to be no intent of interdependencies. The SOSCOE is used to provide commonality in communications.

b. FCS Interoperability

It operates with other systems via contribution (Level 1), coordination (Level 2) and cooperation (Level 3) similarly to today's systems. The SOSCOE facilitates these processes by providing standardization for these processes.

The most important interoperability attributes for FCS are:

- Completeness - all relevant items available, including entities, their attributes, and relationships between them

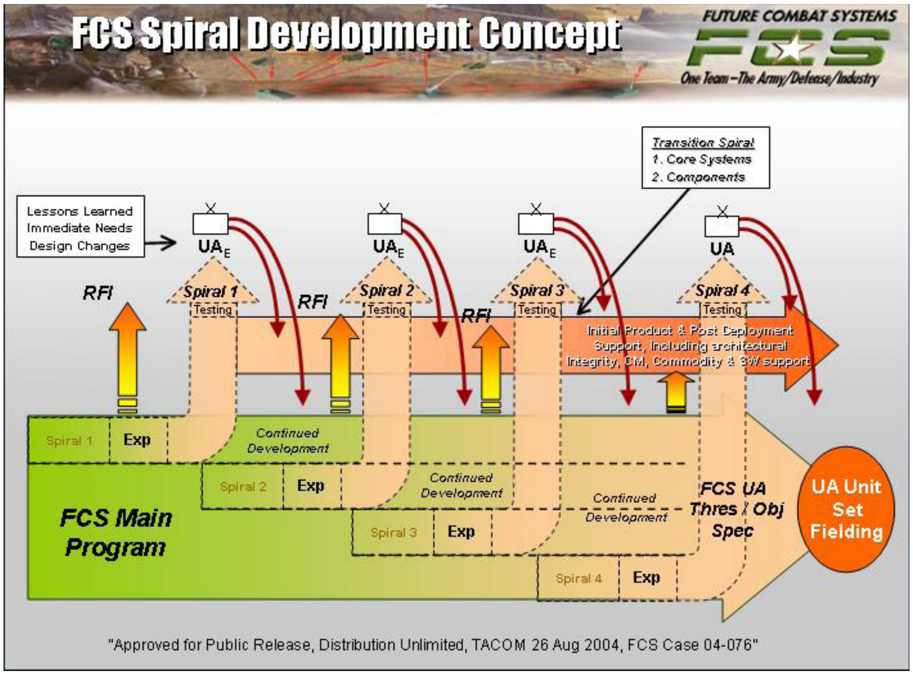
- Correctness - all items in the system faithful representations of the realities they describe
- Accuracy or Level of Precision - dependent on the purpose
- Consistency - across different systems and applications (tailored)
- Connectivity – specified integration of nodes, type of connections, syntactic compatibility, quality of service and bandwidth/data rate requirements
- Capacity – databases, scalability, number and type of applications, processor requirements
- COTS – use of and consideration of obsolescence, instability in standards or availability, security, and reliability

The other attributes are not drivers of CTEs.

c. FCS TRA Requirements and Guidelines

FCS identified their FoS enabled by a SOSCOE up front. They have identified spirals (see Figure 43) and adjustments have been made over time. Unfortunately only 18 of the 49 technologies currently rated have demonstrated TRL 6 and none of the critical technologies may reach TRL 7 until the production decision in fiscal year 2012. Given this is a FoS; only those COE or infrastructure CTE would impact the FCS in the short term; as the FCS should be able to be fielded as systems are ready once a SOSCOE is ready. In the GAO report 06-367 (GAO, 2006) there are 13 related SOCOE networking technologies. The rest are associated with specific functions or systems.

Technology maturation plans have been delayed or not kept up with predicted maturation expectations by 3-5 years in some cases. The Critical Design Review (CDR) is being held two years prior to production; this seems very unrealistic given the advanced hardware technologies in development. The program structure seems to be based on calendar dates not knowledge points (See Figure 44). FCS development status has been the subject of at least two GAO reports for the lack of mature technologies and program structure issues.


FCS Spiral Development Concept

FUTURE COMBAT SYSTEMS FCS One Team – The Army/Defense/Industry

"Approved for Public Release, Distribution Unlimited, TACOM 26 Aug 2004, FCS Case 04-076"

Figure 42. FCS Acquisition Approach [From: Future Combat System Program Office, 2005]

d. FCS CTE Identification

FCS identified 49 CTEs; however, they may not have identified all of them given they have 550 operational requirements and upwards of 11,500 so called SoS level requirements and it is anticipated to have upwards of 90,000 system requirements (GAO, 2006). Requirements are not stable and so by definition the architecture, technology selections may change. This may be mitigated given performance is allowed to be just as good as previous systems not connected via a common network.

The FCS CTEs list is not inclusive of all the programs required by FCS, a total of 52 programs and their associated technologies have been determined to be critical in FCS meeting their required KPPs. Currently, synchronization of schedules is not an option due to the other systems own challenges.

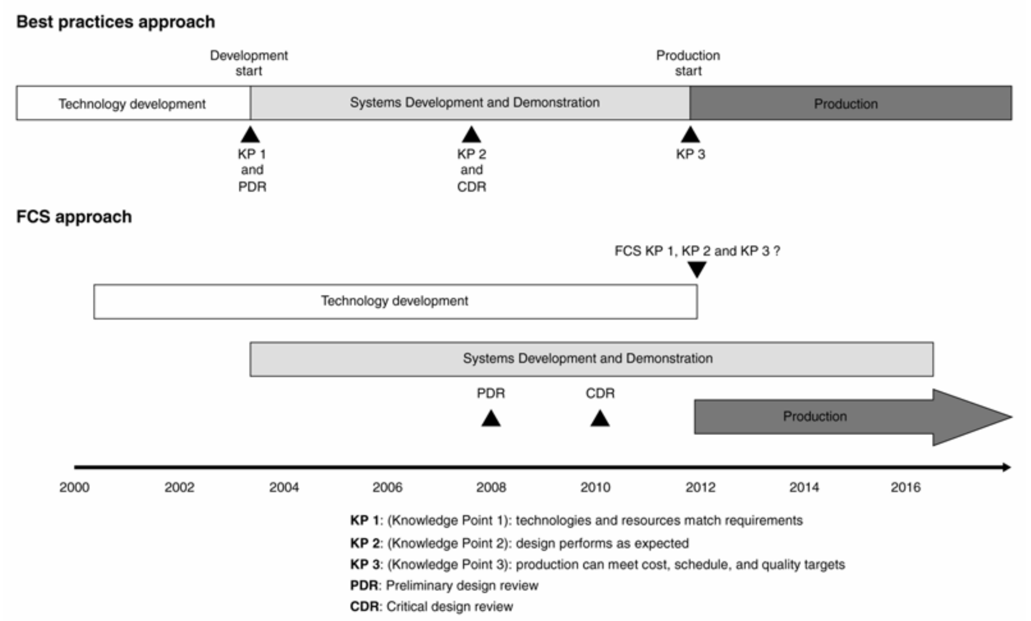

Best practices approach
Development start
Production start
Technology development
Systems Development and Demonstration
Production
KP 1 and PDR
KP 2 and CDR
KP 3
FCS approach
FCS KP 1, KP 2 and KP 3 ?
Technology development
Systems Development and Demonstration
PDR
CDR
Production
2000
2002
2004
2006
2008
2010
2012
2014
2016
KP 1: (Knowledge Point 1): technologies and resources match requirements
KP 2: (Knowledge Point 2): design performs as expected
KP 3: (Knowledge Point 3): production can meet cost, schedule, and quality targets
PDR: Preliminary design review
CDR: Critical design review

Figure 43. FCS approach to integration of COTS technologies [From: GAO, 2006]

e. FCS Technical Challenges

FCS is building new systems. Capability requirements and functional analysis should occur prior to specific system requirements, system functional analysis, and system technology development. They continue to experience system requirements churn even though they are past the System Functional Review. They have spent a lot of time and money to determine allocations of requirements to systems; however, that work is not finished.

FCS is developing a robust modeling and simulation capability; however, with a new type of system (SOSCOE in this case) only a test with the real SOSCOE will show what really happens when used to connect the FoS. It is a definite danger that all CTEs may not been identified given the heterogeneous nature of FCS.

f. FCS Systemic Challenges

FCS is experiencing and will continue to experience a high level of churn given there are more systems outside the FCS umbrella (52 systems) than inside the FCS umbrella (14+1+1) that required to meet the FCS KPPs. The lack of simultaneous system engineering activities, aligned schedules and detailed visibility into the requirements and development and testing of the 52 external essential systems is scary! A time-phased rollout of FCS that is aligned with the maturation and delivery of the external systems is essential. It’s unclear whether the first spiral has included more than can be managed.

3. Army’s Integrated Air Missile Defense Systems of Systems (AIAMD SoS)

Army’s Integrated Air and Missile Defense (IAMD) System of Systems is a capability designed to be deployed as an integrated set of system interoperable and able to synchronize operations with Army, Joint, Interagency, Intergovernmental and Multi-National (JIIM) Net-Centric architectures and systems. The IAMD Battle Command System (IBCS) is designed to be the integrator. (See Figure 45) Common applications via Plug and fight modules are used to interface to legacy sensors, control, and engagement systems (See Figure 46 and 47). The SIAP IABM is part of these plug and fight modules (See next section). The Army adds their service specific common functionality to the plug and fight modules as well. IAMD SoS products are shown in Figure 48.

a. AIAMD SOS, SoS or Not?

FCS is assessed to be a SoS CDP given they are enabled by common processing from SIAP in from their plug-n-fight modules.

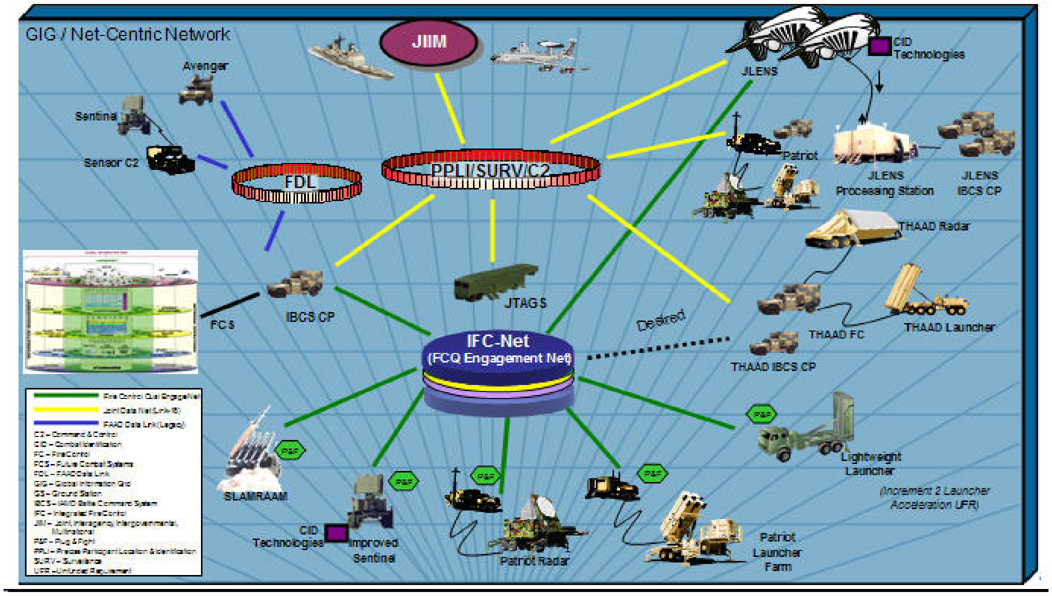


Figure 44. AIAMD SOS Architecture [From: IAMD Program Office, 2007]

b. AIAMD SOS Interoperability

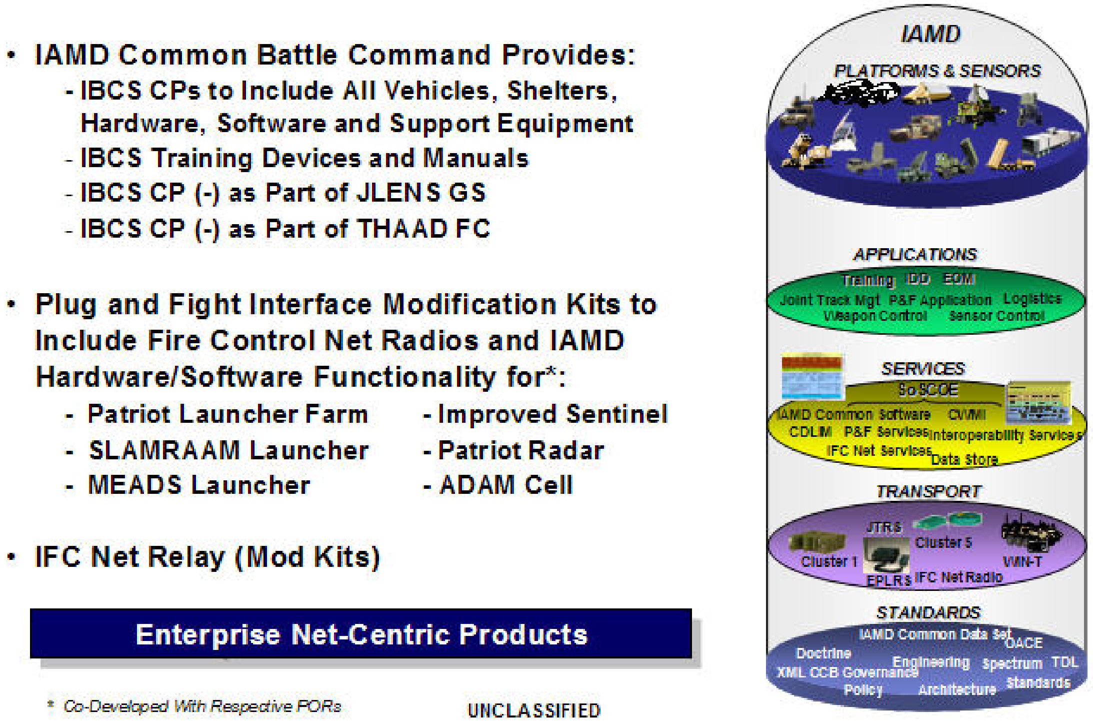
It operates with other external systems via contribution (Level 1), coordination (Level 2), cooperation (Level 3) and collaboration (Level 4) among the systems of the IAMD SoS and the SIAP SoS.

Key interoperability Attributes:

- Completeness - all relevant items available, including entities, their attributes, and relationships between them
- Correctness - all items in the system faithful representations of the realities they describe
- Currency – latency of the items of information
- Accuracy or Level of Precision - dependent on the purpose
- Consistency - across different systems, applications, functions and data/information/knowledge. Note Data models that the SoS is expected to be in compliance with.
- Connectivity – specified integration of nodes, type of connections, syntactic compatibility, quality of service and bandwidth/data rate requirements
- Capacity – databases, scalability, number and type of applications, processor requirements
- COTS – use of and consideration of obsolescence, instability in standards or availability, security, and reliability

c. AIAMD SOS TRA Requirements and Guidelines

AIAMD clearly identified they are a SoS and have made reference to their connection with SIAP. They have identified their detailed schedules (see Figure 49) for spiral one and indicated the functionality for future spirals (see Figure 50).



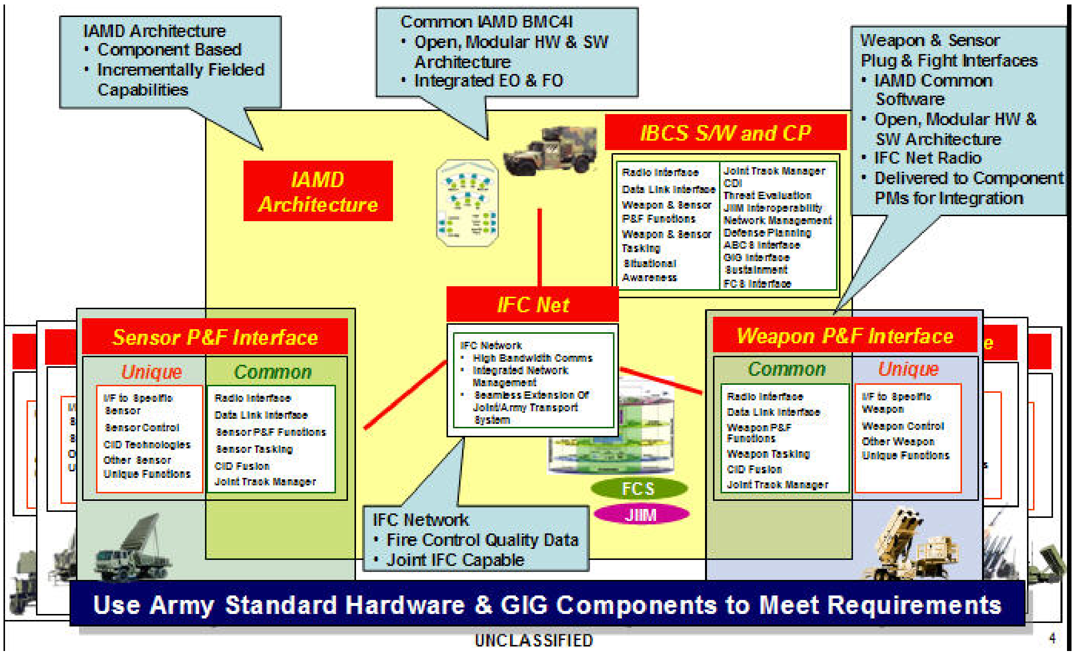
- IAMD Common Battle Command Provides:
  - IBCS CPs to Include All Vehicles, Shelters, Hardware, Software and Support Equipment
  - IBCS Training Devices and Manuals
  - IBCS CP (-) as Part of JLENS GS
  - IBCS CP (-) as Part of THAAD FC
- Plug and Fight Interface Modification Kits to Include Fire Control Net Radios and IAMD Hardware/Software Functionality for*:
  - Patriot Launcher Farm
  - SLAMRAAM Launcher
  - MEADS Launcher
  - Improved Sentinel
  - Patriot Radar
  - ADAM Cell
- IFC Net Relay (Mod Kits)

Enterprise Net-Centric Products

* Co-Developed With Respective PORs

UNCLASSIFIED

Figure 45. AIAMD SoS System Approach [From: IAMD Program Office, 2007]



IAMD Architecture
- Component Based
- Incrementally Fielded Capabilities

Common IAMD BMC4I
- Open, Modular HW & SW Architecture
- Integrated EO & FO

Weapon & Sensor Plug & Fight Interfaces
- IAMD Common Software
- Open, Modular HW & SW Architecture
- IFC Net Radio
- Delivered to Component PMs for Integration

IAMD Architecture

IBCS S/W and CP

Radio Interface Data Link Interface Weapon & Sensor P&F Functions Weapon & Sensor Tasking Situational Awareness	Joint Track Manager CDI Threat Evaluation JIIM Interoperability Network Management Defense Planning ABCS Interface GIG Interface Sustainment FCS Interface

IFC Net

IFC Network
- High Bandwidth Comms
- Integrated Network Management
- Seamless Extension Of Joint/Army Transport System

Sensor P&F Interface

Unique	Common
I/F to Specific Sensor Sensor Control CID Technologies Other Sensor Unique Functions	Radio Interface Data Link Interface Sensor P&F Functions Sensor Tasking CID Fusion Joint Track Manager

Weapon P&F Interface

Common	Unique
Radio Interface Data Link Interface Weapon P&F Functions Weapon Tasking CID Fusion Joint Track Manager	I/F to Specific Weapon Weapon Control Other Weapon Unique Functions

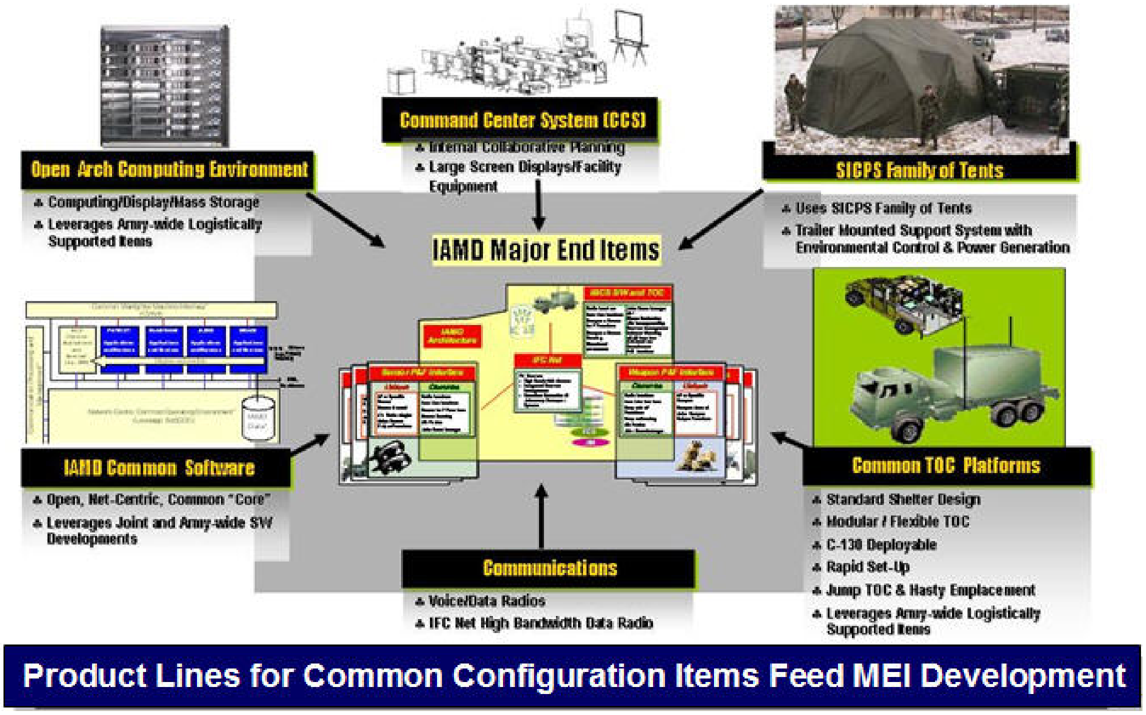
IFC Network
- Fire Control Quality Data
- Joint IFC Capable

Use Army Standard Hardware & GIG Components to Meet Requirements

UNCLASSIFIED

4

Figure 46. AIAMD Plug-n-Fight Interfaces [From: IAMD Program Office, 2007]



Command Center System (CCS)
- Internal Collaborative Planning
- Large Screen Displays/Facility Equipment

Open Arch Computing Environment
- Computing/Display/Mass Storage
- Leverages Army-wide Logistically Supported Items

SICPS Family of Tents
- Uses SICPS Family of Tents
- Trailer Mounted Support System with Environmental Control & Power Generation

IAMD Major End Items

IAMD Common Software
- Open, Net-Centric, Common "Core"
- Leverages Joint and Army-wide SW Developments

Common TOC Platforms
- Standard Shelter Design
- Modular / Flexible TOC
- C-130 Deployable
- Rapid Set-Up
- Jump TOC & Hasty Emplacement
- Leverages Army-wide Logistically Supported Items

Communications
- Voice/Data Radios
- IFC Net High Bandwidth Data Radio

Product Lines for Common Configuration Items Feed MEI Development

Figure 47. AIAMD SoS Product End Items [From: IAMD Program Office, 2006]

Army started the IAMD SoS appropriately and has embarked on technology development. They are reliant on other program managers to develop technologies such as the Warfighter Integrated Network – Tactical (WIN-T) similarly to the FCS program and on SIAP to develop tracking, Combat Identification (CID), and network related algorithms for common distributed processing.

The IAMD SoS has synchronized their internal schedules appropriately; it is unclear how successful they can be with respect to external system development alignment with systems such as WIN-T which currently has several technology issues.

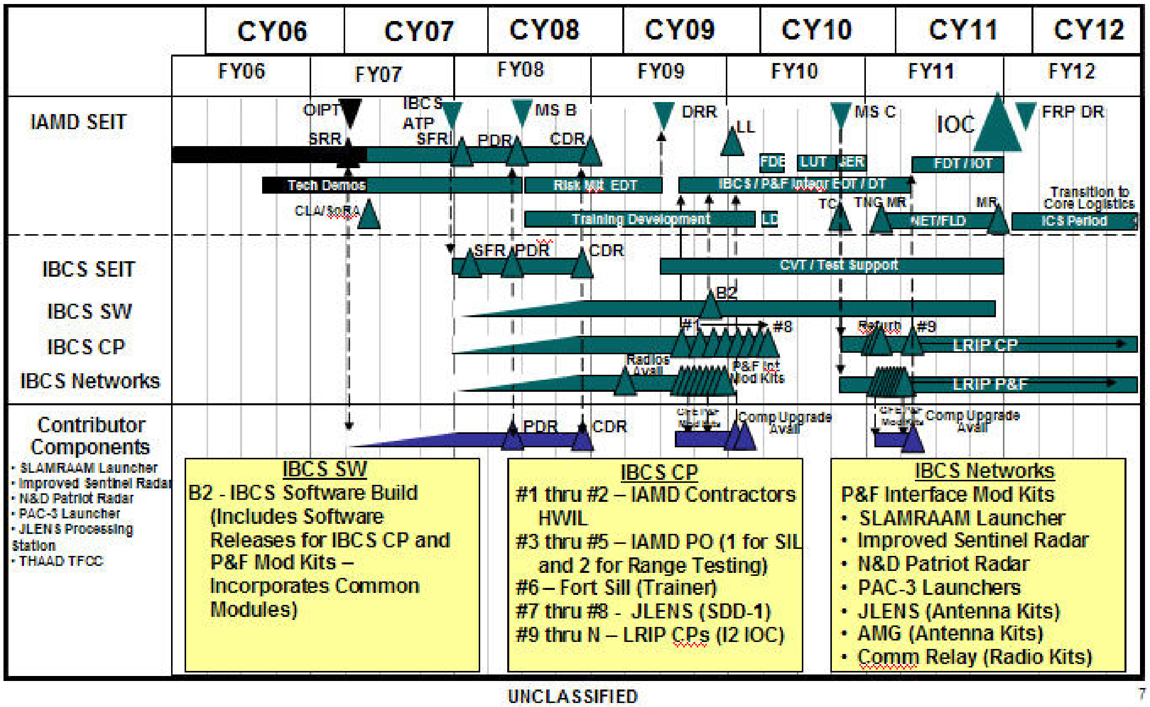
AIAMD SoS will be expecting spiral upgrades in short time cycles than SIAP SoS. SIAP SoS TRA will need to be updated as these spirals are defined and technologies are changed/removed or added.

d. AIAMD CTE Identification

AIAMD SOS has done a good job of identifying CTE for AIAMD and the intersection with SIAP SoS CTEs. It is unclear whether their SoS CTE list includes other essential SoS technologies provided by other programs. The SIAP SoS System Functional Review (SFR) has been held and so risk should be mitigated in this area.

e. AIAMD SOS Technical Challenges

AIAMD is experiencing some challenges given they are part of the SIAP SoS that provides common distributing processing and rely on the ballistic missile defense related technologies from MDA. They have addressed the issue of connecting legacy systems together by using a plug-n-fight module and IBCS approach; this mitigates changes to existing systems.



IBCS SW

B2 - IBCS Software Build (Includes Software Releases for IBCS CP and P&F Mod Kits – Incorporates Common Modules)

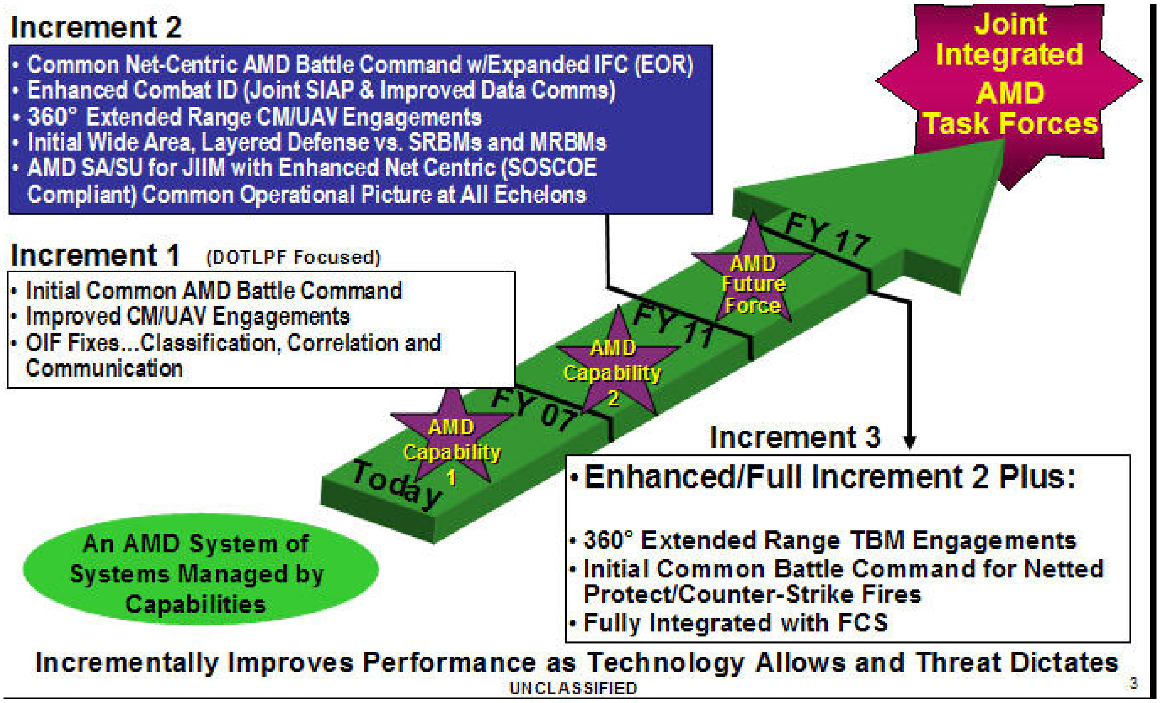
IBCS CP

#1 thru #2 – IAMD Contractors HWIL
#3 thru #5 – IAMD PO (1 for SIL and 2 for Range Testing)
#6 – Fort Sill (Trainer)
#7 thru #8 - JLENS (SDD-1)
#9 thru N – LRIP CPs (I2 IOC)

IBCS Networks

P&F Interface Mod Kits
- SLAMRAAM Launcher
- Improved Sentinel Radar
- N&D Patriot Radar
- PAC-3 Launchers
- JLENS (Antenna Kits)
- AMG (Antenna Kits)
- Comm Relay (Radio Kits)

Figure 48. AIAMD Acquisition Schedule [From: IAMD Program Office, 2007]



Increment 2

- Common Net-Centric AMD Battle Command w/Expanded IFC (EOR)
- Enhanced Combat ID (Joint SIAP & Improved Data Comms)
- 360° Extended Range CM/UAV Engagements
- Initial Wide Area, Layered Defense vs. SRBMs and MRBMs
- AMD SA/SU for JIIM with Enhanced Net Centric (SOSCOE Compliant) Common Operational Picture at All Echelons

Increment 1 (DOTLPF Focused)

- Initial Common AMD Battle Command
- Improved CM/UAV Engagements
- OIF Fixes...Classification, Correlation and Communication

Increment 3

- Enhanced/Full Increment 2 Plus:
- 360° Extended Range TBM Engagements
- Initial Common Battle Command for Netted Protect/Counter-Strike Fires
- Fully Integrated with FCS

Joint Integrated AMD Task Forces
FY 17
AMD Future Force
FY 11
AMD Capability 2
FY 07
AMD Capability 1
Today
An AMD System of Systems Managed by Capabilities

Incrementally Improves Performance as Technology Allows and Threat Dictates

UNCLASSIFIED

3

Figure 49. AIAMD Spiral Development [From: IAMD Program Office, 2007]

They will face issues regarding proper allocation of KPPs to IAMD SoS from both SIAP SoS and IAMD SoS. They are building a representative modeling and simulation environment to include IAMD and SIAP SoS as it related to Army.

f. AIAMD SOS Systemic Challenges

AIAMD SOS may have alignment issues with other programs. They have not gone to a MS B, therefore, these may be able to be worked prior to that event. They are dependent on legacy systems development and integration timelines and may experience some delays in fielding AIAMD SoS. AIAMD SOS has laid out a spiral acquisition so which can mitigates delays; however, AIAMD SOS systems related to air defense likely would have an impact to meeting SIAP SoS KPPs which require common distributed process and networking technologies.

4. Single Integrated Air Picture System of Systems

Single Integrated Air Picture (SIAP) is the product of fused, common, continuous, unambiguous tracks of all airborne objects in the surveillance area. The SIAP OV-1 can be seen in Figure 51. The SIAP is developed from near-real time and real time data, and is scalable and filterable to support situation awareness, battle management, and target engagements. SIAP is created by the collaboration of multiple systems (see Figure 52 – SIAP SoS Boundary). SIAP is accomplished via an Integrated Architecture Behavioral Model (IABM) which when instantiated in a combat system provides for distributed common processing of data/information (see Figure 53 – SIAP Functional Architecture, 54 – SIAP IABM as executable specification into SIAP SoS Systems, and Figure 55 – SIAP IABM instantiation into SoS system). The IABM is built using a Model Driven Architecture™ approach. This mitigates the ambiguity of 'paper' specifications which leads to divergence of implementation. Using the IABM provides for a common distributed process of data for track management, sensor registration, composite tracking and combat ID.

a. SIAP SoS or Not?

SIAP is assessed to be a SoS CDP enabled by IABM.

b. SIAP Interoperability

SIAP is created collaboratively (Level 4) by the systems of the SoS to meet SIAP KPPs. Given that SIAP is an enabling capability the other levels of interoperability didn't seem to apply.

Interoperability Attribute List:

- Completeness - all relevant items available, including entities, their attributes, and relationships between them
- Correctness - all items in the system faithful representations of the realities they describe
- Currency – latency of the items of information
- Accuracy or Level of Precision - dependent on SIAP KPPs
- Consistency - across different systems, applications, functions and data/information/knowledge. Note Data models that the SoS is expected to be in compliance with.
- Connectivity – specified integration of nodes, type of connections, syntactic compatibility, quality of service and bandwidth/data rate requirements

- Capacity – scalability (tailored)

Other interoperability attributes not drivers for the SIAP CTEs.

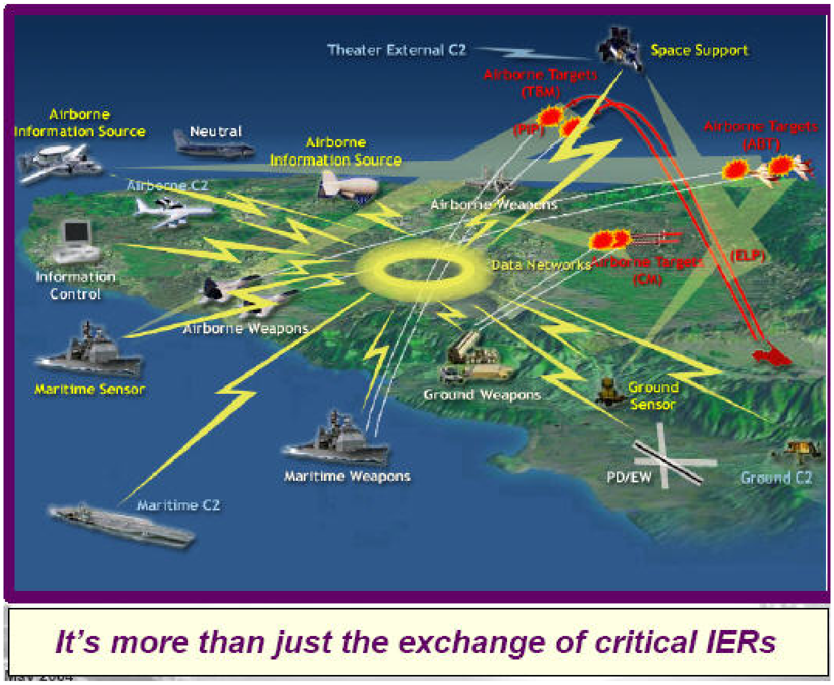
c. SIAP TRA Requirements and Guidelines

SIAP has identified the target systems for instantiation of IABM. The IABM can be used by other SoS as shown by AIAMD SoS. All SIAP CTEs including system specific CTEs of those systems participating in SIAP, for example AIAMD SoS use of WIN-T is required for SIAP are in the SIAP SoS TRA.

SIAP SoS has not yet had its MS B; however, it is anticipated there will be blocks or spirals to add functionality or systems to the SoS. A Joint SoS TRA has been accomplished for SIAP. See Figure 55 for the location and types of CTEs. SoS Engineering has been occurring with all Services and several service programs. PDR is expected to complete in a few months. SoS Test events occur on a regular basis to mature the SoS CTEs.

d. SIAP CTE Identification

SIAP CTEs were identified by representatives from all the services for the SoS unique and specific system CTEs required for participation in SIAP SoS using knowledge of the OVs and SVs and other engineering artifact regarding SIAP. As a system is added to the SoS, the specific system will be reviewed for their specific system CTEs as well.



It's more than just the exchange of critical IERs

Figure 50. SIAP OV-1 [From: Wilson, 2004]

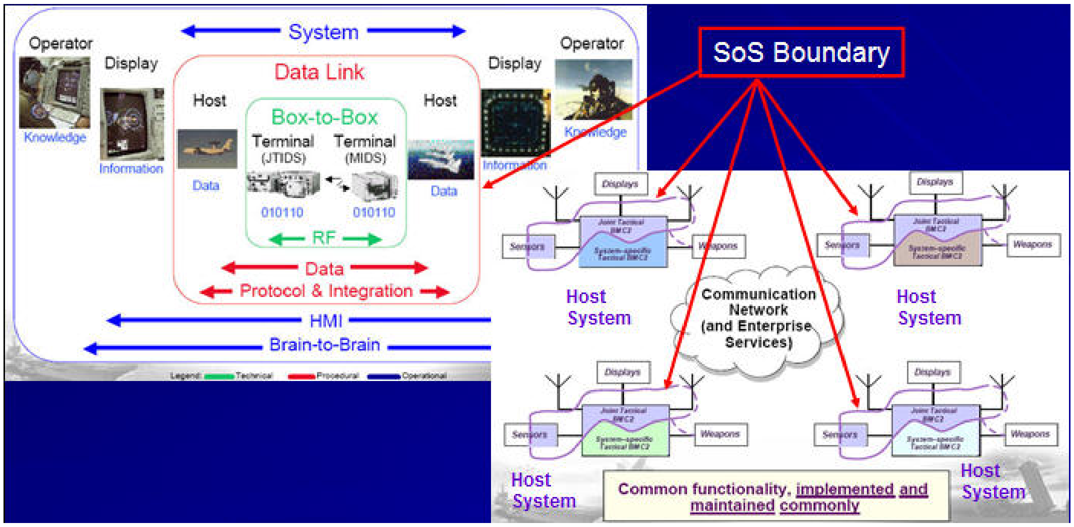
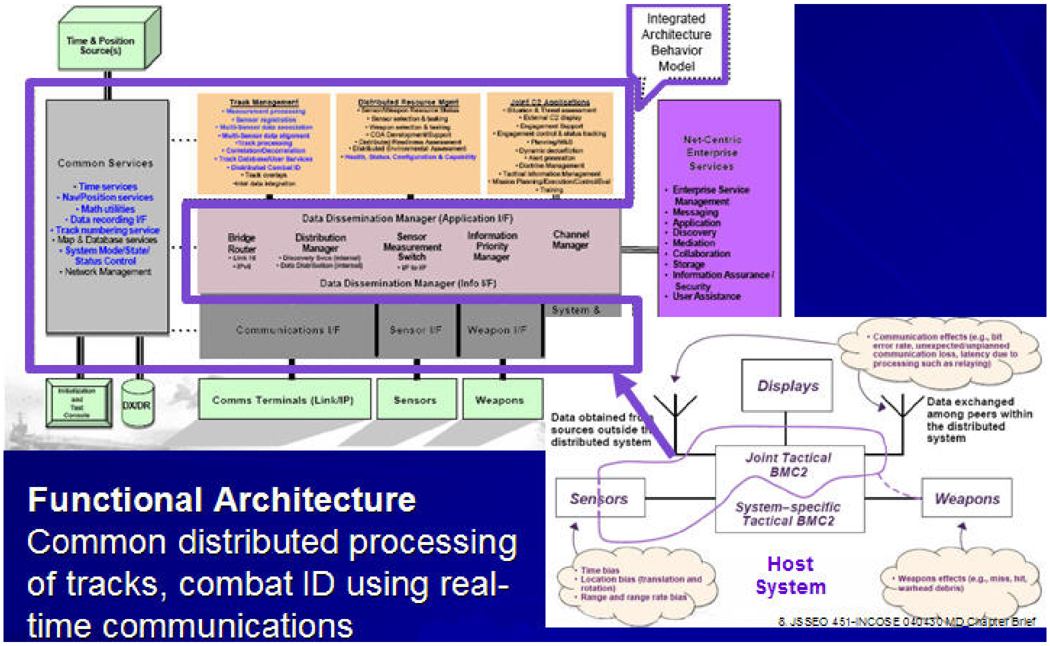


Figure 51. SIAP SoS Boundary [After Ref Wilson, 2004]


Time & Position Source(s)
Integrated Architecture Behavior Model
Common Services
• Time services
• Nav/Position services
• Math utilities
• Data recording I/F
• Track numbering service
• Map & Database services
• System Mode/State/ Status Control
• Network Management
Track Management
• Measurement processing
• Sensor registration
• Multi-Sensor data association
• Multi-Sensor data alignment
• Track processing
• Correlation/Decorrelation
• Track Database/User Services
• Distributed Combat ID
• Track overlays
• Intel data integration
Distributed Resource Mgmt
• Sensor/Weapon Resource Status
• Sensor selection & tasking
• Weapon selection & tasking
• COA Development/Support
• Distributed Readiness Assessment
• Distributed Environmental Assessment
• Health, Status, Configuration & Capability
Joint C2 Applications
• Situation & Threat assessment
• External C2 display
• Engagement Support
• Engagement control & status tracking
• Planning/WLS
• Dynamic deconfliction
• Alert generation
• Doctrine Management
• Tactical Information Management
• Mission Planning/Execution/Control/Eval
• Training
Net-Centric Enterprise Services
• Enterprise Service Management
• Messaging
• Application
• Discovery
• Mediation
• Collaboration
• Storage
• Information Assurance / Security
• User Assistance
Data Dissemination Manager (Application I/F)
Bridge Router
• Link 16
• IPv6
Distribution Manager
• Discovery Svcs (internal)
• Data Distribution (internal)
Sensor Measurement Switch
• IP to IP
Information Priority Manager
Channel Manager
Data Dissemination Manager (Info I/F)
Communications I/F
Sensor I/F
Weapon I/F
System &
Initialization and Test Console
DX/DR
Comms Terminals (Link/IP)
Sensors
Weapons
• Communication effects (e.g., bit error rate, unexpected/unplanned communication loss, latency due to processing such as relaying)
Displays
Data obtained from sources outside the distributed system
Data exchanged among peers within the distributed system
Joint Tactical BMC2
System–specific Tactical BMC2
Sensors
Weapons
• Time bias
• Location bias (translation and rotation)
• Range and range rate bias
Host System
• Weapons effects (e.g., miss, hit, warhead debris)
8. JSSEO 451-INCOSE 040430 MD Chapter Brief

Functional Architecture
Common distributed processing of tracks, combat ID using real-time communications

Figure 52. SIAP Functional Architecture [After Ref Wilson, 2004]

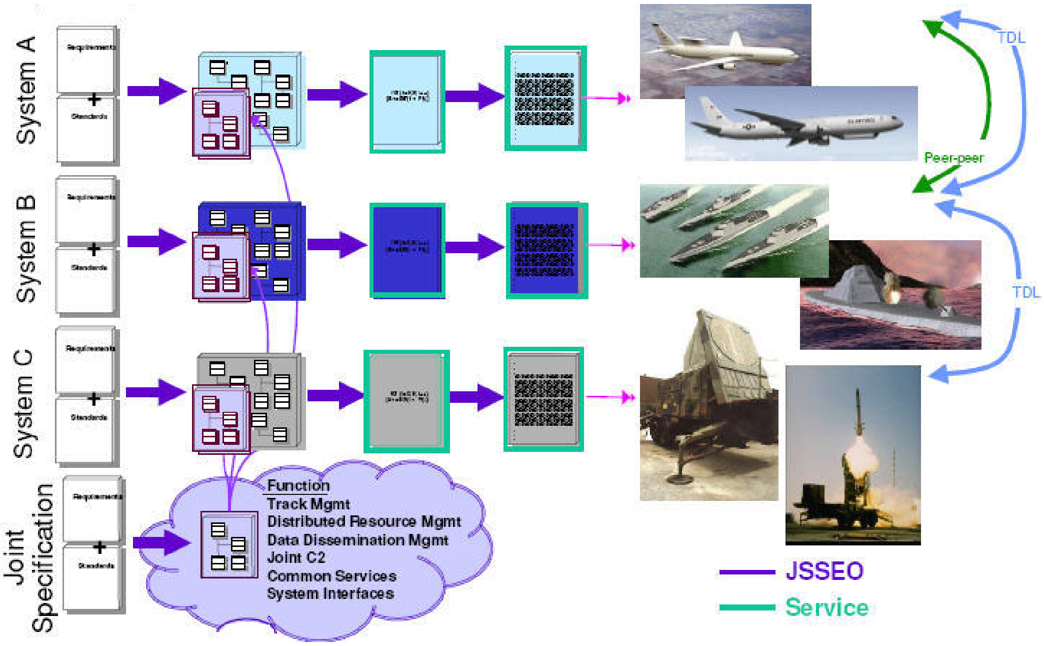


Figure 53. SIAP IABM as executable specification into SIAP SoS Systems [From: Wilson, 2004]

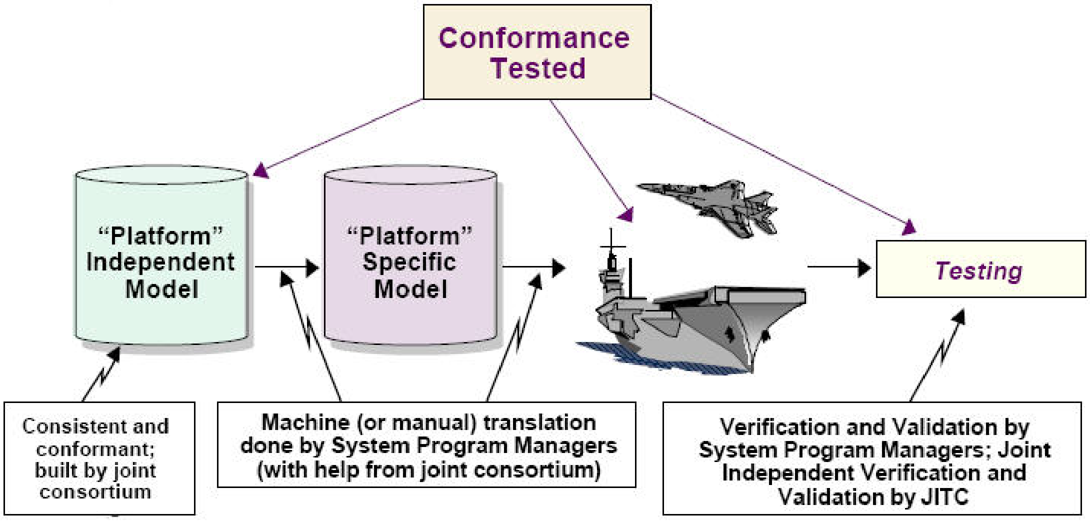

Conformance Tested
"Platform" Independent Model
"Platform" Specific Model
Testing
Consistent and conformant; built by joint consortium
Machine (or manual) translation done by System Program Managers (with help from joint consortium)
Verification and Validation by System Program Managers; Joint Independent Verification and Validation by JITC

Figure 54. SIAP IABM Instantiation into a SIAP SoS system [From: Wilson, 2004]

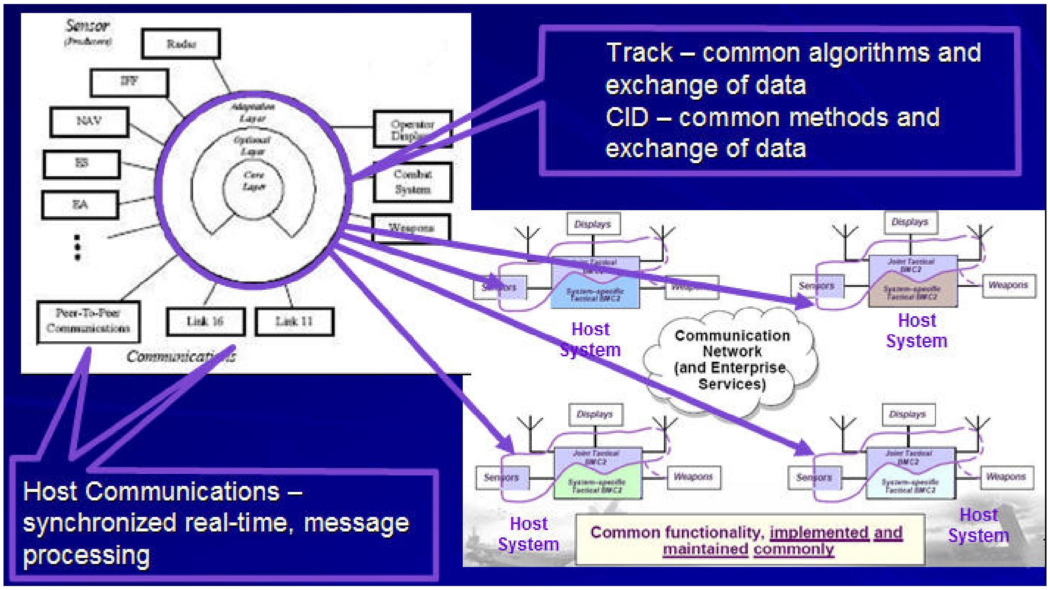

Sensor
(Producers)
Radar
IFF
NAV
ES
EA
Adaptation Layer
Optional Layer
Core Layer
Operator Display
Combat System
Weapons
Peer-To-Peer Communications
Link 16
Link 11
Communications
Track – common algorithms and exchange of data
CID – common methods and exchange of data
Displays
Joint Tactical BMC2
System-specific Tactical BMC2
Sensors
Weapons
Host System
Communication Network (and Enterprise Services)
Host Communications – synchronized real-time, message processing
Common functionality, implemented and maintained commonly

Figure 55. SIAP CTE Locations [After Ref Wilson, 2004]

e. SIAP Technical Challenges

The SIAP KPPs were not finalized until recently and so there was some risk of selecting technologies that wouldn't meet SIAP KPPs; this risk was not realized. KPP allocation to specific systems is problematic and analysis will be ongoing. SIAP

SoS is made up of a mix of new and legacy systems. Work is ongoing to create appropriate modeling and simulation/test venues to cover the diversity of Service systems.

f. SIAP Systemic Challenges

It has been a challenge to have system specific CTEs that are required to meet SIAP KPPs matured in alignment with SIAP SoS schedules. The SIAP SoS was originally structured to only mature the IABM CTEs and not all the SoS CTEs. The SoS KPPs could not be adequately tested beyond TRL 5 without representative systems instantiating the IABM and developing their system specific CTEs for participation in SIAP SoS testing (e.g., radios, sensor algorithms). SIAP will be initially fielded with a small number of systems and as systems are available they will be added.

THIS PAGE INTENTIONALLY LEFT BLANK

IV. PRELIMINARY ANALYSIS

A. APPROACH

Based on the research questions and the literature review, definitions of SoS and types of SoS, a taxonomy for degrees of interoperability, SoS TRA requirements and guidelines and a CTE identification checklist were derived from the literature review and applied during the research phase to four DoD systems that were identified as potential SoS.

Analysis of the research with respect to the research questions are reviewed and analyzed to provide a basis for final conclusions and recommendations regarding SoS TRA requirements and guidelines, SoS definitions and/or type definitions, degree of interoperability definitions, SoS acquisition guidance, and TRL description modifications.

B. SOS TECHNOLOGY READINESS ASSESSMENTS ANALYSIS

1. Relevant Environment

In order to adequately conduct a TRA, the operational relevant environment needs to be characterized. An understanding with regard to type of system and the degree of interoperability are fundamental to understanding the environment. Given the literature review, the proposed system and degree of interoperability definition, four potential SoS were analyzed to determine if these definitions were valid.

a. SoS Definitions and Types

The research showed thatsystems that may be labeled as SoS do not necessarily meet the same SoS definition. The definition of SoS that was used was the following:

System of Systems:

> A set or arrangement of interdependent systems that are related or connected to provide a given capability. The loss of any part of the system will significantly degrade the performance or capabilities of the whole (Chairman of the Joint Chief of Staff, 2007)."

It was found that neither TBMCS or FCS qualify as a SoS, rather a common COE facilitates communication, contribution and cooperation (albeit different COEs).

It was found that AIAMD and SIAP do qualify as a SoSs. These two systems use common distributed processing via embedded algorithms from both SIAP and the IAMD SoS in the plug-n-fight modules and the integrating IBCS. In addition, the SIAP SoS is not predicated on having a COE across the SoS; therefore, just having a COE isn’t a determining factor of whether a program is a FoS, SoS, or other type of system.

There was not enough research performed to determine whether the proposed types of SoS – SOA, COE, and CDP are valid. It was found in this research that having a COE is more of an infrastructure or backbone for communications rather than indicator of collaborative common distributive processing. The FCS program may intend in the future to require synergistic performance increased and include this in their COE. Further research will be required to determine whether SoS SOA or SoS COE are valid specific types of SoS.

Given the definition of SoS and determining what systems are SoS provides the basis for level and type of system engineering and program acquisition planning.

b. Degrees of Interoperability and Interoperability Attributes

The research showed that differing types of systems have different types of interoperability. The definition determined via the literature review and used during the research showed a continuum of interoperability from connectionless through collaborative.

Degrees of Interoperability:	Level 0	Connectionless (self explanatory)
	Level 1	Contribute
	Level 2	Coordinate

Level 3 Cooperate

Level 4 Collaborate

The literature review and research showed that the term collaboration is used colloquially by programs to mean systems are connected in some way without making a distinction as to purpose.

It was found that TBMCS, FCS, and AIAMD SoS all interoperate and perform contribution, coordination and cooperative actions. SIAP SoS was found to mainly support collaboration activities. Given this, it appears useful to designate the degrees of interoperability required rather than defaulting that the highest level of interoperability is characterized the SoS.

The definitions of interoperability facilitated verification of the system type (FoS, SoS, or other) and prepped the research for technology location/identification. It was expected that for each of the interoperability attributes that the degree of interoperability would drive these behaviors. Each system was evaluated with respect to the Interoperability Attribute List (repeated here):

- Completeness - all relevant items available, including entities, their attributes, and relationships between them
- Correctness - all items in the system faithful representations of the realities they describe
- Currency – latency of the items of information
- Accuracy or Level of Precision - dependent on the purpose
- Consistency - across different systems, applications, functions and data/information/knowledge. Note Data models that the SoS is expected to be in compliance with
- Connectivity – specified integration of nodes, type of connections, syntactic compatibility, quality of service and bandwidth/data rate requirements
- Capacity – databases, scalability, number and type of applications, processor requirements
- COTS – use of and consideration of obsolescence, instability in standards or availability, security, and reliability

The research showed the following:

The TBMCS and FCS were not as concerned with currency and consistency as compared with AIAMD SOS and SIAP. Currency and consistency are the key drivers of CTEs for collaborative common distributive processing. In generally all the interoperability attributes are of interest to any system that is communicating with others if cooperating to accomplish a mission or collaborating on the same task.

2. SoS TRAs

a. SoS TRA Requirements and Guidelines

The following SoS TRA requirements and guidelines were developed from the literature review and used during the analysis of the four potential SoS:

1. Clearly describe the type of SoS and degree of interoperability required – (SOA, COE, or CDP) and provide rationale.
2. Indicate which if any of the systems of the SoS is part of another SoS or FoS (name related programs).
3. Identify SoS spirals/blocks or other expected increments and their timeframes including spirals/blocks of specific systems of the SoS. Provide list of expected changes in architecture, performance, functionality and technology.
4. In the SoS TRA include all CTEs required to meet SoS KPPs/operational requirements; include SoS unique CTEs as well as system unique CTEs required for the specific system to participate as a system of the SoS (e.g., a new radio) regardless of who is responsible for funding or developing.
5. Provide an update to the SoS TRA when any of the systems of the SoS are going thru a spiral upgrade independently of the SoS. Each system of the SoS needs to be assessed for any changed technology or technology implementation to assure SoS performance is preserved.
6. SoS Milestones B and C shall be scheduled post system Milestone Bs and Milestone C's for SoS (or at least in the same timeframe, +/- 3 months). Specific systems need to demonstrate TRL 6 and TRL 7 prior to demonstrating SoS TRL 6 and SoS TRL 7.
7. Systems that are part of a SoS shall include SoS CTEs in their system (SoS in the case of a IAMD SoS) specific TRA. Each individual system will need to develop their system specific technologies to a TRL 6 and above as well as demonstrate system functionality with SoS specific technologies to a TRL 6 and above.

8. All SoS CTEs whether part of the SoS or part of the specific systems of the SoS, shall be assessed against SoS requirements. These assessments should begin as early as possible (recommend TRL 3).

In analysis of all four systems, these guidelines were found to be helpful in the analysis with respect to technology readiness. If TBMCS had initially followed these guidelines they would have had an opportunity to determine their system type and started the appropriate engineering up front. It appears that FCS may still not understand the type of system they are building since they indicate they are a FoS enabled by a SoS. They have had significant issues with program structure and technology readiness. They may have more success if they establish their FCS SOSCOE (or just FCS COE) and develop and deploy systems as they are mature.

AIAMD SOS and SIAP appear to be on track with most of the SoS TRA requirements and guidelines. Neither system has pasted MS B; therefore, optimism is probably warranted while declaration of success will be based on results of SOS development and testing.

With regard to the extension of the descriptions at a minimum for TRL 3-9, this will be the subject of follow-on work. In general, it will be recommended to stay consistent with System TRAs and explicitly add language that acknowledges the SoS TRA process that a program must show by analysis and then by demonstration and test in a SoS environment that the CTE are sufficient to meet functionality, behavior and performance wrt the appropriate interoperability attributes in support of SoS KPPs. The author used a combination of the current TRL descriptions, MDA checklist and Nolte's calculator (as a checklist) to conduct a now approved Joint SoS TRA for SIAP in support of an anticipated MS B.

b. SoS Technology Location/Identification

Applying the SoS Technology Location/Identification checklist was not able to be assessed by this research. This list was developed and proposed by the author while the Technology Development Division Chief at SIAP. This checklist was used to identify technology by the SIAP Technology Development team in collaboration with the SIAP SoS systems. Future collaboration with other SoS programs and S&T professional is needed.

3. SoS Acquisition Challenges

SoS, FoS and Enterprise systems have significant challenges given the expectations of increased levels of performance, diversity of systems, and increased degrees of interoperability. SoS Engineering is a necessary and time consuming process required to achieve success. Acquisition planning and timelines, requirements setting, TRA and other acquisition documentation, and proper modeling and simulation/test facilities for SoS should be planned up front to obtain the resources required and set expectations. The following is a summary of the challenges experienced by the four systems analyzed.

a. SoS Technical Challenges

The beginning years of a program are extremely difficult if the system definition and expected degree of interoperability are not set properly. System architecture and engineering activities will not be accomplished (in the case of TBMCS) or be conflicted (in the case of FCS). Requirements churn and failure to include critical systems inside the lifelines of the FoS/SoS will lead to program restructure and failure. FCS has been the subject of GAO reports; this may in fact not be warranted if they concentrated on SOSCOE first and then added systems over time.

System engineering activities with systems outside the lifelines of an Enterprise system FoS or SoS will continue to be a challenge given the scope of external systems and the unaligned acquisition schedules. FCS has 52 programs outside its lifelines that are considered required to meet KPPs and yet they only have 14+1+1 that are inside their lifelines. It was probably challenging to justify program personnel to adequately cover the system engineering activities required to engineer 66+ systems together based on a program of 14+. It’s as if the house is being built and the wiring and plumbing will be designed and installed after the fact.

The JCIDs and CDD process of defining SoS and FoS capability requirements provides opportunity to put together systems in innovative and collaborative ways to meet the requirements; however, the work required to allocate those KPPs appropriately across the SoS is challenging. Its especially challenging when the model and simulation is predicated on system models and simulations of medium to high fidelity which may not be available for sometime after program initiation.

b. SoS Systemic Challenges

Program synchronization appears to be impossible given the number of systems that are required to collaborate unless the DoD acquisition model is fundamentally changed. It's extremely difficult to coordinate inside a Service portfolio and almost impossible across Services or at the Joint level. Given the nature of systems being procured by spiral or blocks, the idea that this level of complexity can actually be engineered and managed with the current state of architecture and engineering tools will take heroic efforts by talented and experienced professionals. TBMCS and FCS indicated they need to at least interface with 76 applications (413 segments) and 170 systems respectfully – one understands given this number why a COE is so important.

Given the requirement for MDAP/MAIS technologies to be certified TRL 6 and the inability to synchronize all the required programs, it may be better to start with less systems, initially have lower performance requirements and build the interoperability infrastructure first. This would provide for less capability with lower risk. The other option is to limit SoS TRA to only the unique CTEs for SoS operations and not expect any SoS certifications until the system MSs. This will increase risk to achieving the SoS possibly leading to delays in the fielding of the SoS as well as a Nunn-McCurdy breach.

THIS PAGE INTENTIONALLY LEFT BLANK

V. CONCLUSIONS AND RECOMMENDATIONS

A. CONCLUSIONS

1. System Definitions

The following definition of SoS from CJCSI 3170 was found to be appropriate for conducting a SoS TRA:

> A set or arrangement of interdependent systems that are related or connected to provide a given capability. The loss of any part of the system will significantly degrade the performance or capabilities of the whole.

The definition was able to be used to distinguish SoSs and non-SoS types of systems. Systems were distinguished by whether or not the set of systems were mutually dependent and whether their performance would degrade, under a condition where there is the minimum number of systems.

A SoS definition is critical to the development of a SoS for determining acquisition strategies and timelines, requirements, required system engineering activities, TRA requirements, acquisition documentation, and proper modeling and simulation/test facilities. SoS engineering will be more complex and time consuming than FoS engineering given that common distributed processing to enable real-time collaboration requires consideration of all systems constraints and restraints within the SoS. The research shows that the lack of the proper distinctions as to type of system can lead to improper funding and time allocations for development. FCS in particular if handled as a FoS vice a SoS would be able to put together a program structure that develops the SOSCOE first and then builds out the FCS by adding systems as they mature. FCS appears to be attempting to do both a FoS and SoS simultaneously which has put the program under undue pressure and assessment. The SOSCOE is an enabler for infrastructure functions and would be better labeled a COE.

Making a distinction of types of SoS may be useful. The current distinctions found in the literature review and those proposed in this thesis do not yet assist in defining the key features of the SoS. Without the key features being defined, the SoS will be at risk of failure during development and testing in an inappropriate operational relevant environment. This occurred for both as TBMCS and FCS.

2. Interoperability Taxonomy

The following defined degrees of interoperability were used in the research where Command and Control/directing was evaluated in the context of the degree of interoperability:

Level 0 Connectionless

Level 1 Contribute - situational awareness primarily for safety or information exchange

Level 2 Coordinate - determination of how and when to share resources

Level 3 Cooperate - determination and plan of how to accomplish related tasks for a common mission

Level 4 Collaborate - determination and work to be done together to accomplish a task

These levels were found to be appropriate for distinguishing degrees of interoperability and were able to be used to verify a SoS or non-SoS. They were useful when combined with the interoperability attributes for identifying and locating technologies in support a TRA. Key to applying these degrees of interoperability was understanding the nature of the required system interactions. If a TBMCS system was passing data to another TBMCS system to support mission planning this was clearly cooperating towards a mission, whereas, in AIAMD SoS the passing of data to support SIAP was clearly a collaboration to determine the air picture via common distributed processing (algorithms). Failure to distinguish the level/degree of interoperability led to the first TBMCS operational tests failing because of an expectation of collaboration vice cooperation.

The literature review showed no agreed to definitions of degrees of interoperability exist. In general, the term collaboration in the literature is used very broadly to mean – any coordinated, cooperative, or collaborative effort. The sense is that collaborative is better than coordinated or cooperative. This broad interpretation and desire to be ‘collaborative’ has the unfortunate effect of strengthening the practice of labeling any set of systems a SoS vice FoS or Enterprise System. As indicated prior, misapplication of SoS to FCS has led to program and engineering challenges. FCS is specifically cited as saying their minimum requirement is to do as well as the present requirement, where systems are not connected via the SOSCOE, leading one to conclude that cooperation is the minimum capability required. The assessment of TRLs in a cooperative environment may not have CTEs associated with armor be in the same list as SOSCOE CTEs such as radios.

This thesis shows that there are no DoD definitions regarding degrees of interoperability even though guidance clearly indicates that interoperability is key to current and future warfighting. Taking steps towards defining the levels or degrees of interoperability would assist in DoD programmatics and systems engineering activities.

3. SoS TRA Requirements and Guidelines

The TRA Deskbook is an excellent guide for conducting TRAs. Adding SoS specific requirements and guidelines would facilitate performing SoS TRAs. The following SoS TRA requirements and guidelines were used during the research to determine if using these guidelines would have benefited the programs analyzed.

1. Clearly describe the type of SoS and degree of interoperability required – (SOA, COE, or CDP) and provide rationale.
2. Indicate which if any of the systems of the SoS is part of another SoS or FoS (name related programs).
3. Identify SoS spirals/blocks or other expected increments and their timeframes including spirals/blocks of specific systems of the SoS. Provide list of expected changes in architecture, performance, functionality and technology.
4. In the SoS TRA include all CTEs required to meet SoS KPPs/operational requirements; include SoS unique CTEs as well as system unique CTEs required for the specific system to participate as a system of the SoS (e.g., a new radio) regardless of who is responsible for funding or developing.

5. The PM should require an update to the SoS TRA when any of the systems of the SoS are going thru a spiral upgrade independently of the SoS. Each system of the SoS needs to be assessed for any changed technology or technology implementation to assure SoS performance is preserved.

6. SoS Milestones B and C shall be scheduled post system Milestone Bs and Milestone C's for SoS (or at least in the same timeframe, +/- 3 months). Specific systems need to demonstrate TRL 6 and TRL 7 prior to demonstrating SoS TRL 6 and SoS TRL 7.

7. Systems that are part of a SoS shall include SoS CTEs in their system (SoS in the case of a IAMD SoS) specific TRA. Each individual system will need to develop their system specific technologies to a TRL 6 and above as well as demonstrate system functionality with SoS specific technologies to a TRL 6 and above.

8. All SoS CTEs whether part of the SoS or part of the specific systems of the SoS, shall be assessed against SoS requirements. These assessments should begin as early as possible (recommend TRL 3). The technology developer should received the SoS requirements that may impact technology development as early as possible.

The SoS TRA requirements and guidelines were found to be appropriate and would have been helpful to the programs analyzed. FCS is not synchronized with system the other systems that are critical to meet its operational requirements. FCS would have been required to have all CTEs at TRL 6 by MS B vice progressing through a CDR without all technologies at TRL 6. Without specific guidelines, each DoD program will approach SoS and FoS differently and each will go through the learning curve without benefit of other programs' lessons learned. The primary difference between these SoS TRA requirements and guidelines vice the ones in the TRA Deskbook is the specifics for what technologies to include in the SoS TRA and the timing of SoS MSs and TRAs. These requirements and guidelines are extensions of a system TRA requirements and guidelines. The biggest impact to a program is that technologies will most likely need to be matured earlier in their program in order to be demonstrated in a SoS environment.

4. SoS Technology Location/Identification Checklist

A SoS technology identification and locator checklist was proposed from the literature review and used during the research analysis. The SoS checklist is focused on identification and location of technologies based on interoperability attributes and architecture and system engineering artifacts. This checklist and Nolte's TRL calculator was used by the author during SoS TRA activities for SIAP and was found to be useful in identifying and locating technologies within each of the systems of the SoS. An example, it was used during the research to evaluate available FCS's engineering artifacts, this led to the conclusion that the CTE list may be incorrect given the systems may only be required to be cooperative (vice collaborative).

The literature is rich with SoS architecture assessment approaches, these coupled with Nolte's TRL calculator can be used for developing a SoS technology identification/locator checklist. The author is interested in future collaboration with other SoS programs and S&T professionals to determine and develop a technology identification and location checklist for SoS.

5. SoS Acquisition Challenges

Technical challenges include a) performing SoS engineering activities prior to system engineering activities and many SoS are assembled from legacy systems, b) KPPs for a capability are not easily allocated to individual systems, c) appropriate SoS relevant environment modeling and simulation and test and evaluation environments will typically be built post system design and development, d) identification of SoS CTEs, and e) SoS are typically enabled with software which is easily changed. Given these challenges, the technology development and acquisition strategies for the researched potential SoS were assessed for their ability to be employed for SoS technology maturation given the challenges of synchronization.

The research showed that SoS architecture, technology development and engineering activities need to be in alignment in order to reduce the risk to the SoS development. Identification, location and development of common elements and common distributed processing require SoS engineering upfront by all parties involved.

TBMCS found that they were able to make progress once requirements were set and system engineering activities were formalized. FCS is in the process of determining final system requirements and their program has be restructured to reflect the systems that are maturing in the first spiral. IAMD SOS and SIAP are being synchronized and SoS modeling and simulation and test events are being put in place to properly demonstrate and test to SoS requirements. Without these adjustments to these programs, the programs would experience failure.

There is not enough research or data to analyze regarding how the performance of systems of a SoS together will meet the SoS KPPs/operational requirements. More research will need to be accomplished as these systems are developed and tested.

There is not enough research or data to analyze the effect of spiral or block development on SoSs. Configuration control and management will be key to the success in this area.

SoS architecture, engineering and a SoS TDS will be key to developing SoS technologies. Innovation in S&T and acquisition strategies will be required to successfully develop SoS.

Systemic challenges within the DoD include: a) critical technology developed by the individual programs are in alignment with their respective schedules not the SoS program schedule, b) SoS technology selections and development prior to completion of capability engineering and then individual system(s) engineering drives up risk; SoS engineering needs to be at least through System Functional Review prior to a MS B decision, and c) it's challenging to test the critical technologies in an integrated manner if the individual systems have not had the opportunity to all develop their systems enough to have representative systems for SoS testing (e.g., relevant environment for a integrated heterogeneous distributed system) and d) the fielding of a SoS capability is typically time-phased over several years in capability spirals or increments with differing sets of systems and services.

The AIAMD SoS and SIAP program are moving towards aligned system schedules for key systems. The other systems of these SoS have been phased to occur at later dates. Direction and funding was applied to SIAP systems up front to perform the required SoS engineering activities including accomplishing a SoS System Functional Review and SoS Preliminary Design Review. AIAMD SOS and SIAP included key systems only for the first spiral of their respective SoS. The SoS engineering accelerated system architecture and engineering activities for the systems of the SoS; however, the development of technologies and systems was not able to be accelerated due to the funding levels being normally phased later for the systems. This impacts the ability to perform SoS technology demonstration without up-front planning.

System development occurs in alignment with system program plans and funding; this puts the schedules for SoS Developmental Testing (DT) and Operational Test and Evaluation (OT&E) post the systems DT and OT&E. Some systems will achieve a system Initial Operating Capability (IOC) prior to the SoS IOC. SoS DT events will need to take place prior to approving a limited fielding of the system's SoS capability. After an initial synchronization of system schedules, follow-on spirals or blocks will most likely be out of synchronization with follow-on spirals or blocks of the other systems of the SoS. It is anticipated that the AIAMD and SIAP schedules which are synchronizing during the first spiral will be unsynchronized for subsequent spirals. For COEs, the research shows that they can be developed and then systems which conform to the COE standards and protocols can be phased with little impact.

System engineering activities with systems outside the programmatics of a SoS will continue to be a challenge given the scope of external systems and the unaligned acquisition schedules. TBMCS, FCS and AIAMD SOS have a number of significant technologies being developed outside of their program cycles and this synchronization issue doesn't appear to have been successfully addressed. Research is required to determine when and if a SoS is really required. Also, research is required to determine if architectures, standards and protocols if implemented properly will mitigate the need to have SoS which are tightly coupled in order to accomplish task synchronization.

Based on the research it is recommended that a SoS be formally initiated with requirements and designated technology development and acquisition strategies. Funding and direction should be provided to all programs required to participate in the SoS to accomplish SoS architecture and engineering activities prior to system development. Implementation by all the systems may be able to be time-phased.

SoS Milestones B and C shall be scheduled post system Milestone Bs and Milestone C's (or at least in the same timeframe, +/- 3 months). Systems need to demonstrate TRL 6 and TRL 7 prior to demonstrating SoS TRL 6 and SoS TRL 7.

B. RECOMMENDATIONS AND FUTURE RESEARCH

1. System Definitions

It is recommended that all of DoD adopt the same SoS and FoS definitions and that USD(AT&L) use these definitions in their DAG, TRA Deskbook, SoS Engineering Guide and other S&T and acquisition directives and instructions. This would provide for commonality of efforts and expectations for SoS technology development and acquisition.

Further research and definition into the types of SoS should be pursued given normally one size doesn't fit all, this would enable proper SoS program planning and execution.

2. Interoperability Taxonomy

It is recommended that DoD, including the Chief of the Joint Chiefs of Staff and USD(AT&L) develop and adopt a common taxonomy for degrees of interoperability in acquisition guidance in support of the JCIDS process. It is recommended that the degree of interoperability taxonomy be based on nature of the communications to support mission and common tasks and subsequently required performance be defined in terms of the Interoperability Attributes (e.g., accuracy, latency).

Also, it is recommended that the Milestone Decision Authority determine and designate require key OVs and SVs be accomplished prior to MS decisions.

3. TRAs Requirements and Guidelines

It is recommended that DUSD(S&T) include specific SoS requirements and guidelines in the TRA Deskbook. Adding SoS specific requirements and guidelines would facilitate performing and evaluating SoS TRAs. Also, it is recommended that as SoS types are identified that these are included in the TRA Deskbook vice the current listing of IT systems.

Also, the TRL descriptions do not currently describe SoS aspects. It is recommended that specific language is added regarding recommended SoS demonstrations and testing in the descriptions for both hardware and software TRL.

4. SoS Technology Identification/Location Checklist

A SoS technology identification and locator checklist was proposed from the literature review and used during the research analysis. It is recommended that a SoS checklist be developed in collaboration with other SoS programs and S&T professionals to determine and develop a technology identification and location checklist for SoS. Nolte's calculator is a great start towards such a tool. This checklist would be a useful to include in an appendix of the TRA Deskbook.

5. SoS Technology Development and Acquisition Strategies

It is recommended that the Milestone Decision Authority hold a formal Program Initiation meeting to start technology development for SoS unique technologies and to begin SoS architecture and engineering activities with the requisite direction and funding. It is recommended that all anticipated systems be directed to participate in the SoS architecture and engineering activities and then time-phase these systems (no big bang with tens of systems). In addition, it is recommended that if a COE is needed that it be engineered first, prior to development of systems that use the COE. Also, it is recommended that SoS Milestones B and C are scheduled post systems Milestone Bs and Milestone C's (ok if in the same timeframe, +/- 3 months).

It may be that defined architectures, standards and protocols if implemented properly would mitigate the need to have tightly coupled systems such as a SoS that requires common distributed processing. It is recommended that research be conducted to determine what SoS are truly needed and when COE, FoS or Enterprise System would meet warfighting requirements, since SoS acquisition is challenging and expensive.

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF REFERENCES

Alberts, D. S., Garstka, J. J., & P. Stein, Frederick P. (1999). *Network Centric Warfare: Developing and Leveraging Information Superiority* (Second (Revised) ed.) CCRP Publications.

Alberts, D. S., Hayes, R. E., & Signori, D. A. (2001). *Understanding Information Age Warfare* CCRP Publications.

Assistant Secretary of Defense for Networks and Information Integration/Department of Defense Chief Information Officer (2004). *Department of Defense Instruction Procedures for Interoperability and Supportability of Information Technology (IT) and National Security Systems (NSS) number 4630.8.*

Bilbro, J. (2006). *Systematic Assessment of the Program/Project Impacts of Technological Advancement and Insertion*.

Boardman, J., & Sauser, B. (2006). System of Systems - the Meaning of Of. *Proceedings of the 2006 IEEE/SMC International Conference on System of Systems Engineering*.

C4ISR Architecture Working Group. (1997). *C4ISR Architecture Framework version 2.0.*

Carnegie Mellon Software Engineering Institute. Retrieved August 2007 www.sei.cmu.edu.

Chairman of the Joint Chief of Staff, J8. (16 March 2007). *Joint Capabilities Integration and Development System, CJCSI 3170.01E*.

Child, J. (2006). *Program Update Future Combat System*.

Christiansen, B. (2005). Shared Tactical Pictures Using a SOS Approach.

Collens Jr, Josiah R., & Krause, B. (2005). *Theater Battle Management Core System Systems Engineering Case Study*.

Collens Jr., Josiah R. (2005). *Theater Battle Management Core System: Lessons for Systems Engineers*.

Deputy Under Secretary of Defense for Science and Technology (DUSD(S&T)). (May 2005). *Department of Defense Technology Readiness Assessment (TRA) Deskbook.*

Dickerson, C., & Soules, S. (2002). *Using Architecture Analysis for Mission Capability Acquisition*.

DiMario, M. (2006). System of Systems Interoperability Types and Characteristics in Joint Command and Control. *Proceedings of the 2006 IEEE/SMC International Conference on System of Systems Engineering*.

Frazier, G. (2001). *The DII COE: An Enterprise Framework.*

Future Combat System Program Office. *Future Combat System Overview*. Retrieved August 2007 www.army.mil/fcs/.

Future Combat System Program Office. (2005). *Future Combat System 2005 Flipbook.*

GCCS-AF Team (2006). *GCCS-AF SOA brief*.

Gold, R., & Jakubek, D. (2005). *Technology Readiness Assessments for IT and IT-Enabled Systems*.

Government Accountability Office. (1999). *BEST PRACTICES: Better Management of Technology Development Can Improve Weapon System Outcomes* No. GAO/NSIAD-99-162.

Government Accountability Office. (2005). *Defense Acquisitions: Assessments of Selected Major Weapons Programs* No. GAO-05-301.

Government Accountability Office. (2006). *Improved business case is needed for future combat System's successful outcome* No. GAO-06-367.

Habayeb, A. R. (2005). Architecture-based Systems Engineering and Integration. (8th Annual Systems Engineering Conference.

Hanratty, J. M. (2007). *Technology Transition Metrics*.

Headquarters ACC/DOYS. (1996). *Air Combat Command Concept of Operations for Theater Battle Management Core Systems*.

IAMD Program Office. (2006). *IAMD Program Overview for RFI 28 AUG 2006.*

IAMD Program Office. (2007). *Integrated Air and Missile Defense Program Overview to Industry Day 15 March 2007.*

Institute of Electrical and Electronics Engineers, Inc. (1994). *P1220 Standard for Application and Management of the Systems Engineering Process.*

Institute of Electrical and Electronics Engineers, Inc. (2002). *IEEE 610.12-1990 Standard Glossary of Software Engineering Terminology*.

Joint Chiefs of Staff. (12 April 2001 as amended through 13 June 2007). *Joint Publication 1-02 Department of Defense Dictionary of Military and Associated Terms*.

Joint Chiefs of Staff. (14 May 2007). *Joint Publication 1-01 Doctrine for the Armed Forces of the United States*.

Joint Chiefs of Staff. (20 March 2006). *Joint Publication 6-0 Joint Communications System*.

Joint Chiefs of Staff. (2002). *Global Combat Support System Family of Systems Requirements Management Structure*.

Kasunic, M., & Anderson, W. (2004). *Measuring Systems Interoperability: Challenges and Opportunities* No. CMU/SEI-2004-TN-003) Carnegie Mellon, Software Engineering Institute.

Maier, M., & Rechtin, E. I. (2002). Chapter 7 Collaborative Systems. *The Art of Systems Architecting* (Second ed.,) CRC Press LLC.

Mandelbaum, J. (2005). Enabling Technology Readiness Assessments (TRAs) with Systems Engineering. (NDIA 8th Annual Systems Engineering Conference 2005).

Mandelbaum, J. (2007). Technology Readiness Assessment brief. (Technology Maturity Conference 2007).

Mankins, J. C. (1995). *Technology Readiness Levels, A White Paper, April 6, 1995*.

Merriam-Webster. *Merriam-Webster Online Dictionary*. Retrieved August 2007 http://www.m-w.com/game/index.htm.

Missile Defense Agency. *MDA/DV Hardware Maturity Checklists for Technology Readiness Levels (TRLs)*. Retrieved August 2007 http://www.dodsbir.net/solicitation/sbir073/mda073.pdf.

National Aeronautics and Space Administration. *NASA Software Technology Readiness Levels*. Retrieved August 2007 http://www.esdswg.org/softwarereuse/Resources/trls/.

Nolte, W. (2004) *Technology Readiness Level Calculator V 2.2* (Ver 2.2 ed.).

Norman, D. (2004). *Engineering a Complex System: The Air and Space Operations Center (AOC) as a Complex System Exemplar*.

Norman, D., & Kuras, M. L. (2004). *Engineering Complex Systems*.

Powell, C. (2006). Key Issues and Requirements in System-of-Systems (SoS) for High-Throughput Battlespace Information Fusion and Persistent Surveillance. (2nd Conference System of Systems Engineering).

Sauser, B., Ramirez-Marquez, J., Verma, D., & Gove, R. (2006). *Determining System Interoperability Using an Integration Readiness Level Brief*.

Sauser, B., Ramirez-Marquez, J., Verma, D., & Gove, R. (2006). From TRL to SRL: The Concept of Systems Readiness Levels. (Conference on Systems Engineering Research).

Siel, C. (2006) System of Systems Engineering Conference brief, 2006.

Subramanian, M. (2000). *Network Management: Principles and Practice* Addison Wesley.

The Internet Engineering Task Force. Retrieved August 2007 www.ietf.org.

National Defense Act Authorization 2006, TITLE VIII--ACQUISITION POLICY, ACQUISITION MANAGEMENT, AND RELATED MATTERS, House Conference Report 109-360, (2006).

Title 10 USC §2433 Unit Cost Reports, (2006).

Under Secretary of Defense for Acquisition, Technology and Logistics. (2006). *Defense Acquisition Guidebook*.

Under Secretary of Defense for Acquisition, Technology and Logistics. (2006). *Systems of Systems (SoS) Systems Engineering Guide: Considerations for Systems Engineering in a System of Systems Environment*.

United States Joint Forces Command. (2004). *The Joint Warfighting Center Joint Doctrine Series pamphlet 5*.

Wikipedia®. *Wikipedia® - communication*, Retrieved August 2007 http://en.wikipedia.org/wiki/Communication.

Wilson, J. (2004) *Integrated architecture development and fielding brief to INCOSE MD Chapter*.

Zavin, J. (2005). Net-centricity & Net-ready - Beyond Technical Interoperability & C4ISR.

INITIAL DISTRIBUTION LIST

1. Defense Technical Information Center
   Ft. Belvoir, Virginia

2. Dudley Knox Library
   Naval Postgraduate School
   Monterey, California

3. Dr. Meng
   Naval Sea Systems Command
   Washington, District of Columbia

4. Single Integrated Air Picture Program Manager
   Single Integrated Air Picture Joint Program Office
   Arlington, Virginia

5. Mr. Robert Gold
   Deputy Under Secretary for Defense, Science and Technology
   Washington, District of Columbia

6. Dr. Jay Mandelbaum
   Institute for Defense Analyses
   Arlington, Virginia